total cost for handling in-app transactions should it decide not to impose any fees on transactions between a Developer and User made through linked out-of-app payment options (as provided for in this Section) and not to impose any fees on in-app transactions using Alternative In-App Payment Solutions (as provided for in Section III.B) in a given year.

13. Section III.A of the Proposed Injunction prohibits Google from creating barriers to Developers' ability to offer Users the option to complete their would-be in-app transactions outside the app, using payment solutions other than Google Play Billing.

14. As discussed above, the DDA's anti-steering provision makes it more difficult for Developers to effectively offer out-of-app purchases that use non-Google payment methods as alternatives to in-app purchases that use Google Play Billing. Google could continue to dissuade Developers from using those alternatives if it were allowed to limit how Developers can communicate with Users about them; Sections III.A.1-2 address these concerns by prohibiting any limitations on the form of communication or its content.

15. Similarly, Google could limit competition from out-of-app purchasing options if it were allowed to restrict how Developers may invoke those alternatives—e.g., if Google could degrade the user experience of using an out-of-app purchase option. Section III.A.3 of the Proposed Injunction would prohibit such actions by Google.

16. Finally, Section III.A.4 is intended to ensure that Google cannot use its distribution market power to "tax" transactions between a Developer and User made outside of the app at a level that would prevent equally-efficient or more-efficient out-of-app payment options from competing with Google on the merits. Public disclosure of Google's average per-transaction total costs for handling in-app transactions is necessary so that developers and competitors know whether Google is offering them fees that comply with the Injunction, and only by having access to this information can they monitor Google's compliance.

17. The provisions of Section III.A would encourage the development of web-based payment solutions that can be used for out-of-app purchases. As discussed above, such solutions are currently poor substitutes for Android In-App Payment Solutions in part because of Google's

restrictions. As I testified at trial, without those restrictions, Developers could significantly streamline the process of linking an app to a web-based out-of-app purchase option.[32]

18. The provisions of Section III.A do not restrict Google from competing on the merits in the market for Android In-App Payment Solutions. These provisions impose no requirements on Google regarding what features it may offer in Google Play Billing, how it may communicate with Users and Developers about Google Play Billing's relative merits, or how it may price its own services (other than to forbid price structures that prevent equally-efficient or more-efficient out-of-app payment options from competing with Google on the merits). Moreover, these provisions do not require Google to do anything new; instead they require it *not* to do certain things. Therefore, compliance imposes no obvious material costs on Google.

B. NO TYING OF DISTRIBUTION TO PAYMENTS

III.B. <u>No Tying of Distribution to Payments (Contractual, Economic or Technical)</u>: Google shall not enforce any existing agreement, enter into any new agreement or otherwise engage in any conduct that requires the implementation of GPB in any Android app, including, but not limited to, enforcing Sections 1 and/or 2 of its Google Play Payments Policy.

1. **Google shall not enforce or enter into contractual provisions, guidelines or policies, or impose technical restrictions or financial terms, that (a) restrict, prohibit, impede, disincentivize or deter Developers from integrating any Alternative In-App Payment Solution, whether alongside GPB or in lieu of GPB; or (b) restrict, prohibit, impede, disincentivize or deter Developers from offering different prices for in-app purchases using GPB and any Alternative In-App Payment Solution and/or making that price difference visible to Users.**
2. **Google shall not require Developers to use Google APIs (such as Google's "User Choice Billing" APIs) in order to invoke Alternative In-App Payment Solutions.**
3. **Google shall not impose any Coercive Fees on transactions made through Alternative In-App Payment Solutions.**

19. Section III.B of the Proposed Injunction would prohibit Google from coercing Developers into using Google Play Billing by imposing barriers on the use of Alternative In-App Payment Solutions. This section prevents Google from requiring the use of Google Play Billing in any

---

[32] Tadelis Testimony, Tr. 2557:4-18.

Android app, regardless of the means that Google might use to impose such a requirement: contractual, economic, or technical. As I testified at trial, severing the tie will encourage entry, reduced fees, and increased innovation in the market for Android In-App Payment Solutions.[33]

20. Specifically, Section III.B.1 prohibits Google from imposing barriers to Developers' use of Alternative In-App Payment Solutions alongside or instead of the Google Play Store, whether through contract, guidelines or policies, technical restrictions or financial terms. For example, if Google were to require that digital goods sold through an Alternative In-App Payment Solution must be offered at the same price as goods sold through Google Play Billing—or if Users were not informed of the relative prices until after choosing a payment solution—that would inhibit the competitiveness of Alternative In-App Payment Solutions. Section III.B.1(b) prevents such strategies.

21. Section III.B.2 prohibits Google from requiring the use of Google APIs to implement Alternative In-App Payment Solutions, so as to avoid a situation where Google can degrade the user experience of invoking an Alternative In-App Payment Solution.

22. Section III.B.3 is intended to ensure that Google cannot use its distribution market power to "tax" in-app purchases using Alternative In-App Payment Solutions at a level that would prevent equally-efficient or more-efficient Alternative In-App Payment Solutions from competing with Google on the merits (as Google currently does under User Choice Billing).

23. As discussed above, offering User Choice Billing as Developers' only alternative to using Google Play Billing exclusively (as the States' Settlement allows) is an insufficient remedy to address the coercive tie. User Choice Billing requires that Google Play Billing be offered alongside any alternative payment mechanism.[34] In contrast, the Proposed Injunction would sever the tie by preventing Google from deterring Developers from integrating their chosen in-app payment solution in lieu of GPB.[35]

---

[33] Tadelis Testimony, Tr. 2566:1-8.

[34] Loew Testimony, Tr. 3162:9-23.

[35] Proposed Injunction, III.B.1. *See also* Tadelis Testimony, Tr. 2561:5-2566:17.

24. The provisions of Section III.B do not restrict Google from competing on the merits in the market for Android In-App Payment Solutions. These provisions impose no requirements on Google regarding what features it may offer in Google Play Billing, how it may communicate with Users and Developers about Google Play Billing's relative merits, or how it may price any of its own services (other than to forbid price structures that prevent equally-efficient or more-efficient Alternative In-App Payment Solutions from competing with Google on the merits). Moreover, like the provisions of Section III.A, these provisions specify only what Google may *not* do and therefore impose no obvious material costs on Google.

C. NO DISCRIMINATION ON THE BASIS OF PAYMENT SOLUTION CHOICE

III.C. <u>No Discrimination on the Basis of Payment Solution</u>:

1. **Google shall not reject for distribution, or otherwise disadvantage, any Android app submitted for distribution through the Google Play Store on the basis of the app's actual or intended integration of one or more Alternative In-App Payment Solutions, whether alongside GPB or in lieu of GPB.**
2. **Google shall not retaliate or threaten to retaliate against any Developer on the basis of such Developer's actual or intended integration of one or more Alternative In-App Payment Solutions into its app(s), whether alongside GPB or to the exclusion of GPB.**
3. **Google shall not enforce any existing agreement, enter into any new agreement or otherwise engage in any conduct that imposes financial terms, technical limitations or otherwise restricts, prohibits or impedes access to the Android platform, any Android functionality and/or features or APIs, to any Android app (including any Third-Party App Stores) or Developer based on whether or not GPB is used by that app or that Developer as a payment solution exclusively or alongside Alternative In-App Payment Solutions.**
4. **Google shall not enforce any existing agreement, enter into any new agreement or otherwise engage in any conduct that conditions or impedes access to, restricts the use of, or conditions the terms of access to any of Google's products or services based on whether or not an Android app or a Developer chooses to use GPB as a payment solution exclusively or alongside Alternative In-App Payment Solutions.**

25. Section III.C of the Proposed Injunction would prohibit Google from making Developers' terms of access to Google Play Store app distribution, the Android platform and Android functionality conditional on their use of Google Play Billing.

26. Section III.C.1 prohibits Google from conditioning in any way a Developer's *equal* access to the distribution services offered by the Google Play Store on the basis of that Developer's choice of payment solution for handling in-app sales of digital goods. In other words, under the Proposed Injunction, Google's distribution services must be payment-solution-agnostic.

27. Section III.C.2 prohibits Google from retaliating or threatening to retaliate against a Developer for use of an Alternative In-App Payment Solution, such as by removing or threatening to remove a Developer's apps from the Google Play Store. In other words, under the Proposed Injunction, Google cannot punish Developers for electing to use Alternative In-App Payment Solutions.

28. Dr. Bernheim has explained the importance to Developers of access to APIs generally, and to Google's proprietary Android APIs specifically.[36] Even if Google is prohibited from tying Google Play Billing to the Google Play Store, it could still coerce the use of Google Play Billing by withholding key Android functionality from Developers who do not use Google Play Billing exclusively. Section III.C.3 of the Proposed Injunction addresses that possibility. It will allow Developers to select an Alternative In-App Payment Solution without sacrificing app capabilities. This, in turn, will allow competitors to Google Play Billing to access the market on a more equal footing than they could in the absence of Section III.C's provisions.

29. Dr. Bernheim has also explained the importance to Developers of access to Google's broad suite of apps and services, such as Google Search and Google Ads.[37] Section III.C.4 prevents Google from restricting access or degrading these services if a Developer chooses to use an Alternative In-App Payment Solution. By allowing Developers to select an Alternative In-App Payment Solution without sacrificing these products and services, Section III.C.4 will allow competitors to Google Play Billing to access the market on a more equal footing.

---

[36] Bernheim Statement, Section III.C; Bernheim Report, ¶¶ 33-47.

[37] Bernheim Statement, Section III.C.

30. The provisions of Section III.C do not restrict Google from competing on the merits in the market for Android In-App Payment Solutions. These provisions impose no requirements on Google regarding what features it may offer in Google Play Billing, how it may communicate with Users and Developers about Google Play Billing's relative merits, or how it may price any of its own services (other than to forbid discriminatory treatment of Developers based on their choice of in-app payment solution). Moreover, like the other provisions of Section III that I have already discussed, these provisions specify only what Google may *not* do and therefore impose no obvious material costs on Google.

D. GOOGLE IS ALLOWED TO COMPETE ON THE MERITS

Notwithstanding the preceding prohibitions, nothing in this Section III shall prohibit Google from engaging in bona fide competition on the merits with respect to in-app payment solutions for Android apps, such as:

1. **Making price or quality improvements to GPB to differentiate it from Alternative In-App Payment Solutions.**

2. **Communicating to OEMs, Carriers, Developers and Users regarding any purported quality or price advantages of GPB over Alternative In-App Payment Solutions, or otherwise publicly promoting GPB.**

31. As I testified at trial, Google's tie prevents other providers from fairly competing in the market for Android In-App Payment Solutions; without healthy competition, fees are higher than they would otherwise be, and Google lacks an incentive to offer needed innovations.[38] The conclusion to Section III of the Proposed Injunction reinforces that Epic asks the Court to establish the conditions for healthy competition in this market. Healthy competition implies—contrary to the present reality in this market—that all providers, including Google, are free to offer innovative products at attractive prices. The provisions quoted immediately above emphasize that Section III of the Proposed Injunction in no way limits Google's ability to compete fairly in the market for Android In-App Payment Solutions.

---

[38] Tadelis Testimony, Tr. 2534:2-18.

Respectfully submitted,

Steven Tadelis, Ph.D.
April 11, 2024

EXHIBIT H

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION THIS DOCUMENT RELATES TO *Epic Games, Inc. v. Google LLC et al.*, Case No. 3:20-cv-05671-JD	Case No. 3:21-md-02981-JD

STATEMENT OF B. DOUGLAS BERNHEIM

APRIL 11, 2024

- Paragraph II.A.4 prevents Google from placing restrictions on developers' ability to offer differentiated content on competing app stores.[29]
- Paragraph II.A.5 prevents Google from prohibiting the withdrawal of apps from the Google Play Store without Google's consent.[30]

(17) An effective remedy must also preclude alternative strategies through which Google could potentially achieve the same objective if parity provisions are disallowed. One possibility is that Google might enter into agreements with developers that require the exclusive distribution on Android of key Android apps and content through the Google Play Store. Paragraph II.A.3 explicitly precludes that conduct.[31]

(18) A second possibility is that Google might use its control of Google Android functionalities and key Android-related products and services to punish developers who explore alternative app distribution methods.[32] The proposed remedy addresses this possibility in two ways:

- Paragraph II.C.1 mandates that Google provide parity access to Android functionalities for alternative Android app distribution channels, or apps downloaded through those channels.[33]
- Paragraph II.C.2 prevents Google from conditioning the use of Google products or services on a developer's actual or intended use of an alternative app distribution channel.[34]

II.C. An effective remedy must prevent Google from imposing frictions on "off-Play" app installations

(19) Evidence presented at trial showed that Google's restrictions on direct downloading and downloading from third-party app stores enhanced its ability to monopolize the Android app distribution market.[35]

---

includes "[m]aking price or quality improvements to the Google Play Store to differentiate it from Alternative Android App Distribution Channels…" Proposed Injunction, 10.

29 Proposed Injunction, ¶ II.A.4.

30 Proposed Injunction, ¶ II.A.5; *see also*, Koh Testimony, Tr. 467:20–469:16 (confirming the non-removal requirement in Exhibit 153, the ABK Project Hug agreement); 482:13–483:9 (confirming the non-removal requirement in Exhibit 162, the Riot Games Project Hug agreement); Bernheim Report, ¶ 335.

31 Proposed Injunction, ¶ II.A.3.

32 I discuss the importance to app developers of access to APIs generally, and to Google's proprietary Android APIs specifically, in Bernheim Report, ¶¶ 33–47.

33 Proposed Injunction, ¶ II.C.1.

34 Proposed Injunction, ¶ II.C.2.

35 Bernheim Testimony, Tr. 2389:1–2393:19 (discussing evidence of effects of Google installation frictions from Epic installation funnel data and OnePlus preinstallations, and concluding that Google's degradation of the download experience enhances Google Play's market power in the market for app distribution); Morrill Testimony, Tr. 169:21:170:6 (testifying that 11 percent of users who tried to download the Amazon Appstore through the unknown sources install flow actually succeeded); Rosenberg Testimony, Tr. 1216:23–1217:2 (discussing Exhibit 682, a slide deck showing how Google recognized that as a result of the unknown sources warning the hurdles were too high for

As I discussed in my report, such restrictions "diminished the success of competing app distribution initiatives."[36]

(20) While Google should not be prevented from imposing legitimate security warnings to protect the safety of Android users, such warnings should not discriminate among apps based on the app store from which users download them, or discriminate against stores based on whether they are pre-loaded or obtained from the web. Prof. Mickens testified at trial that Google's unknown sources flow imposes frictions that are not commensurate with the risk from directly downloaded apps.[37] He proposed an alternative involving (i) a one-time user permission for an installer app to download other apps, and (ii) a warning plus an option to abort the download of any app that has not passed an automated malware check.[38] He also testified that Google could ensure app security by notarizing apps itself in a manner similar to the mechanism used by Apple on Mac computers, or by using third-party verification services such as those Google already employs for secure communication through its Chrome browser, Gmail, and other web services.[39] Finally, he testified that his proposals would make Android no less secure than it currently is, and might make it safer.[40]

(21) Paragraphs II.B.1 and II.B.2 address this conduct by prohibiting Google from imposing unnecessary frictions to disincentivize users from obtaining apps outside of the Google Play Store, while still allowing Google the flexibility to block or impose frictions on apps or app stores that are known malware or are associated with developers who do not obtain proper notarization.[41]

---

most users to install the Amazon Appstore); Kochikar Testimony, Tr. 746:3–752:11 (discussing Exhibit 5718, which describes an 18-step process for installing the Amazon Appstore through the unknown sources install flow); 752:20–756:3 (discussing Exhibit 1517, her email to Jamie Rosenberg in which she described the experience of getting Fortnite on Android via direct downloading as "frankly abysmal" due in part to the 15 steps required); 759:10–761:10 (discussing Exhibit 917, a document she authored that says that "we know that [the install friction] will dramatically limit [Epic's] reach"); 762:19–763:2 (explaining how where there is friction, people fall out and do not complete purchases); Pichai Testimony, Tr. 1360:19–1362:24 (testifying that the steps involved in direct downloading are examples of frictions; the more friction there is, the less likely the user completes the flow).

36 Bernheim Report, Section VI.B.3.

37 Mickens Testimony, Tr. 2114:10–15.

38 Mickens Testimony, Tr. 2148:18–2157:5.

39 Mickens Testimony, Tr. 2157:6–2163:2.

40 Mickens Testimony, Tr. 2163:3–2164:1. Similarly, Google's Dave Kleidermacher testified that (i) trusted third parties could authenticate apps, (ii) Google has introduced a security review badge on the Google Play Store for certain apps that undertake voluntary security review with the App Defense Alliance, and (iii) Google can or could use various technological tools to distinguish safe apps from malware. Kleidermacher Testimony, Tr. 1706:22–1712:1.

41 Proposed Injunction, ¶¶ II.B.1 and II.B.2.

II.D. An effective remedy must reestablish an even playing field to compensate for past harms to competition

(22) As discussed in Section II.B, network effects in app distribution tend to reinforce and perpetuate the market power Google acquired and maintained illicitly.[42] Consequently, even if a remedy broadly prevented Google from engaging in the types of anticompetitive conduct the jury found to be illegal, Google's past conduct would still have a substantial and continuing impact on competition in Android app distribution. Mitigating the future effects of Google's past conduct requires additional remedial measures.

(23) Competing app stores face a chicken-and-egg problem: enticing a significant number of users to consider an alternative to Google Play is challenging without a comparably comprehensive catalog of apps, and compiling such a catalog is challenging without a large base of users.[43] An app store can certainly attempt to build its user base through preload deals, direct downloading, and agreements with developers to offer exclusive content. However, all these measures are limited: the effects of preload deals are gradual because users tend to keep their mobile phones for several years; even simplified forms of direct downloading are considerably less convenient than preloading; and the benefits of offering exclusive content are transitory.[44] Given the market power that Google has maintained for years, a small app store faces hurdles for building a large and stable user base over a relatively short time frame, and its value proposition for developers is difficult to establish. And without the engagement of developers, the likelihood of building the user base becomes even more remote.

(24) Epic's proposed remedy attempts to address these difficulties in three ways. For a period of six years:

- Paragraph II.D.1 allows competing app stores to access Google Play's app catalog "through a background process similar to the Alley Oop integration offered by Google to certain third-party Developers."[45] Google Play would still be allowed to earn revenue from its apps distributed in this way.[46]

---

42 I discussed network effects in my expert report. *See* Bernheim Report, ¶ 455.

43 Bernheim Report, ¶ 455.

44 Preloading on new devices is not likely to have widespread immediate effect on competition as users replace their phones every 2-3 years and preloads are not available on old devices. *See* Bernheim Testimony, Tr. 2434:2-11 (testifying that people buy a new phone "on average once every 2.7 years"); *see also* Lockheimer Testimony, Tr. 1500:3-7 (testifying that people replace phones every two or three years).

45 Proposed Injunction, ¶ II.D.1.i. I understand that Alley Oop denotes a mechanism by which Google Play acts as the backend to another developer's app-distribution efforts, *e.g.,* through an in-app ad. *See, e.g.,* Exhibit 136-043. Google describes Alley Oop as an "inline install solution powered by [Google] Play." Exhibit 1546-007. For a period of 15 months (six-month agreement extended by nine months), Google allowed Facebook to install its apps and others' apps outside of Google Play using Alley Oop. Exhibit 1546-007. *See also*, Bernheim Report, n. 1117; Bernheim Reply Report, n. 1238.

46 Apps distributed in this way "shall be governed by the Google Play Store's distribution agreements with Developers,"

- Paragraph II.D.2 allows distribution of competing app stores on the Google Play Store.[47]
- Paragraph II.D.3 prohibits Google agreements with OEMs or carriers that mandate or incentivize placement of the Google Play Store in any specific location on an Android device.[48]

(25) The first portion is critical because it ameliorates the chicken-and-egg problem by uncoupling the two sides of the market. The Alley Oop strategy allows rival app stores, for a limited period of time, to offer comprehensive catalogs on day one, and consequently lowers an obstacle (which was exacerbated by Google's past conduct) to those rival app stores' being able to compete for users on a more even playing field. A store that succeeds in acquiring users through attractive pricing, superior search features, user-friendly interfaces, and the like, will then be well-positioned to engage developers directly and persuade them to launch their apps in the store's own catalog. The network externalities that sustain Google Play's dominance would thereby be mitigated at least to some degree. At the end of six years, the stores that offer the best value propositions have a better prospect of attaining sufficient user bases and proprietary catalogs to compete without further access to the Google Play catalog.

(26) The second portion of this remedy streamlines the process of acquiring new users but does not directly address the network externalities that protect the market power Google acquired and maintained illicitly. While distribution competitors can under the terms of the proposed injunction self-distribute their stores, Google's years of imposing frictions on direct downloads have trained users to rely on the Google Play Store to the exclusion of direct downloads, and as a result it will likely take some time to make them comfortable with direct downloading. Similarly, while distribution competitors ought to be able to reach agreements with OEMs to preinstall their app stores, that process would only impact the app distribution market with some delay—the large installed base of existing phones relative to new phones means that a substantial portion of Android users would be initially inaccessible through preloading deals. To make competing stores more readily accessible and visible to users, the Proposed Injunction requires Google, for a limited period, to make these stores available through the Google Play Store. Though the Google Play Store's policy of refusing to distribute competing app stores is not part of the conduct that the jury found to be illegal, and there are good reasons to be cautious about requiring the Google Play Store to carry competing stores in perpetuity, this temporary remedy for Google's other misconduct will help accelerate the transition to a more competitive Android app distribution market.

(27) The third portion provides competing app stores with temporary and limited opportunities to offset the Google Play Store's illicitly acquired incumbency advantages with users by negotiating

---

but Users can transfer update ownership to a third-party app store if and when an app becomes available there. Proposed Injunction, ¶ II.D.1.i, ii.

47 Proposed Injunction, ¶ II.D.2.

48 Proposed Injunction, ¶ II.D.3.

comparable or more prominent placement. It does not, however, prohibit an OEM from placing the Google Play Store prominently if, in its judgement, its mobile phone offerings are thereby improved.

(28) An important feature of these remedies is that they neutralize some of the advantages Google acquired through past anticompetitive conduct by enhancing the value competing app stores can offer users and developers, rather than by meaningfully impairing Google's ability to serve these constituencies. The benefit to users and developers is therefore direct with no significant risk of negative consequences to their interests.

II.E. Impact of States' Settlement

(29) Before the trial began, plaintiff States and a class of app consumers reached a settlement with Google regarding Google's anticompetitive conduct. I have reviewed the States' Settlement to determine whether it adequately accomplishes the goals of preventing Google from engaging in future anticompetitive conduct and undoing the effects of Google's past anticompetitive conduct. On the first point, the States' Settlement does not fully prohibit the conduct found to be anticompetitive at trial; neither does it adequately prevent Google from modifying that conduct to achieve the same anticompetitive objectives in a somewhat different way. On the second point, the States' Settlement makes no attempt to undo the effects of Google's past anticompetitive conduct.

(30) With regard to preventing Google from "foreclosing, impairing, and/or disincentivizing pre-installation of alternative app stores through agreements with OEMs" (Section II.A. above), the States' Settlement does not preclude the full menu of anticompetitive provisions that Google has deployed or could deploy in its agreements with OEMs. The States' Settlement prohibits agreements with OEMs that (i) secure preload or home screen exclusivity for the Google Play Store,[49] (ii) prevent OEMs from granting installer rights to preloaded applications,[50] or (iii) require OEMs to obtain Google's permission to preload a third-party app store.[51] That is, if an OEM decides to develop an alternative app distribution channel, the States' Settlement prohibits some, but not all, of the strategies through which Google could hamstring that initiative. Specifically, the States' Settlement does not prevent Google from signing agreements, such as the RSA 3.0 revenue-sharing provisions, that disincentivize OEMs from preloading or featuring alternative app stores.[52] Furthermore, it does not explicitly prevent Google from penalizing an OEM for pre-loading a third-party app store by

[49] States' Settlement, Section 6.6.

[50] States' Settlement, Section 6.7.

[51] States' Settlement, Section 6.8.

[52] The States' Settlement also allows Google to enter into or enforce existing agreements with OEMs that provide it with non-exclusive placement rights on the home screen or any other screen. *See* States' Settlement, Sections 6.6.

B. Douglas Bernheim

April 11, 2024

Date

EXHIBIT I

THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION THIS DOCUMENT RELATES TO: *Epic Games, Inc. v. Google LLC et al.* Case No. 3:20-cv-05671-JD	Case No. 3:21-md-02981-JD Judge: Hon. James Donato

STATEMENT OF MATTHEW GENTZKOW

MAY 2, 2024

functionality of the Google Play Store."[87] To the contrary, Epic's proposed injunction severely constrains the specific security measures that Google may use, and it would undermine security in at least four ways.

61. First, the prohibition on "disincentivizing" sideloading would prevent Google from providing accurate information to users about security risks. For example, informing a user that enabling sideloading increases the risk of malware could reduce the user's incentive to sideload.

62. Second, the proposed remedy would prevent Google from using the full range of signals available to identify, block, and/or warn users about potentially harmful apps or app stores. Any app or app store that had at some point been submitted to any "notarization-like process" would become immune from additional security warnings or safeguards, even if the notarization-like process was known to be imperfect or unreliable, the app or app store had been modified since it was submitted to that process, and/or the app had a combination of features including its source, developer characteristics, code features, and pattern of past behavior that indicated it could pose a significant risk. The only exception would be if it was "known" to be malware. Google would furthermore be prohibited from using the source of an app as a predictor of its security risks.

63. Third, the proposed remedy appears to require that the install flow for downloading apps from the open web using a browser such as Google Chrome or Microsoft Edge be limited to a "single one-tap screen" with "neutral language" asking the user to confirm an app installation, or otherwise be "commensurate" with the installation process for apps from Play.[88] Major browsers, including Google's Chrome browser and Microsoft's Edge browser, provide users with a security warning prompt at the time of download.[89] Dr. Mickens testified in his deposition that these browser warnings are reasonable and that he was not proposing removing them.[90] The proposed injunction appears to require that

---

87 Bernheim Statement, ¶ 55.

88 Epic's Proposed Injunction, II.B.1-2.

89 "Google Chrome Blocks Some Downloads," *Google Chrome Help*, https://support.google.com/chrome/answer/6261569?hl=en, accessed April 10, 2024 ("Chrome automatically blocks dangerous downloads and protects your device and accounts from malware or viruses. … You can always choose to download a file after you receive a warning from Chrome, but take download warnings seriously."); "Microsoft Edge Support for Microsoft Defender SmartScreen," *Microsoft Learn*, January 12, 2024, https://learn.microsoft.com/en-us/deployedge/microsoft-edge-security-smartscreen, accessed April 10, 2024 ("Microsoft Defender SmartScreen determines whether a downloaded app or app installer is potentially malicious based on many criteria … . Files with a known safe reputation will download without any notification. Files with a known malicious reputation show a warning to let the user know that the file is unsafe and has been reported as malicious…. Files that are unknown show a warning to let the user know that the download doesn't have a known footprint and advise caution … Not all unknown programs are malicious, and the unknown warning is intended to provide context and guidance for users who need it[.]").

90 Deposition of James Mickens, *In re Google Play Store Antitrust Litigation*, 3:21-md-02981-JD, March 22, 2023, 162:12-164:4 ("Q. Do you think it was a good design decision for browser vendors to include the

Google remove such warnings from Google's Chrome browser, which is inconsistent with Epic's own expert's opinions, and would prevent Google from displaying warnings that communicate to users the risks of installing apps from the open web, such as websites that falsely purport to have legitimate apps.

64. Fourth, the proposed remedy would limit how OEMs could compete with each other on security by forcing all OEMs to the lowest common denominator. OEMs have the flexibility to customize security features on Android.[91] Restricting OEMs' ability to enact more stringent prompts than the defaults would limit OEMs' ability to compete on security.

65. The economic impact of the proposed remedy would hinge on the details of the "generally available, distribution-channel-agnostic notarization-like process" that would be left as the sole mechanism for protecting Android users from harmful apps.[92] What this process or processes would be, who would provide them, what standards they would have to meet, how they would be monitored, and so on are all left completely unspecified. These details would presumably have to be filled in and overseen by the Court.

66. Even if those details were specified, the versions of notarization that Epic proposed at trial—centralized and decentralized notarization—would bring additional security risks that Dr. Bernheim has not addressed.[93]

---

warning we see in step 2? A. It's reasonable to the extent that the downloading of an APK file is sort of different in terms of ramifications than the downloading of a picture let's say. Q. So you do think it was a good design decision for browser vendors to include this warning; right? A. Well, I think that in this case, there is a decision that browser makers are making here with respect to the potential risk of an action….So to the extent that this warning is actually commensurate with risk, it's a good idea."); 304:4-305:7 ("Q. By virtue of the fact the browser has permission to install apps, you would entirely dispense with any warning from the operating system informing the user that they are about to install an app; is that right? A… So, for example, if you're particularly worried about, for whatever reason, a particular installer app accidentally triggering an installation flow, that type of screen could be added.").

91 Declaration of David Kleidermacher in Support of Google's Objections to Proposed Injunction, *In re Google Play Store Antitrust Litigation*, 3:21-md-02981-JD, May 1, 2024 ("Kleidermacher Declaration"), ¶ 11 ("Android OEMs also have the ability to innovate on security issues and safeguard their users from sideloading risks. To the extent that Epic's proposed injunction applies to OEMs, it would prevent OEMs from providing users with additional security features and protections.").

92 Epic's Proposed Injunction, II.B.2.ii.

93 Qian Trial Testimony, 2240:20-2241:2 ("Q. What was your overall conclusion based on the information that Professor Mickens provided? A… [A]fter some careful analysis, I've arrived at the conclusion that the proposals are less flexible, would introduce new security risks, and impose burden on Google"); 2242:10-17 ("Q. Now, would implementing centralized notarization be a significant change in the design of the Android operating system? A. Yes, it would be a significant change…[t]here's actually profound ramifications on the entire Android ecosystem on all the stakeholders. Right? It doesn't just affect Google. It affects also the OEMs, the users, and developers."); 2244:15-2246:1 ("Q. And, Professor Qian, are there security risks associated with this proposal of centralized notarization?... A. … First, it's possible that after an app has been approved it's going to turn malicious at a later point in time…if Google has previously approved an app, generated a token for that app, it doesn't mean that app is going to be safe forever…Google would have to

67. Providing a notarization service would be costly.[94] Economic principles imply that Google would charge a price for that service in a competitive market and that this would enhance efficiency. Dr. Mickens, Epic's security expert, acknowledged that Google could charge for its services.[95]

68. If Google were asked to provide a service like this to developers without charge, it would essentially be required to offer for free the core security screening and verification services of Play, and to put its own reputation on the line. This would allow another form of free riding that would substantially undermine the Android platform as discussed in **Section II** above.

69. As security is a key dimension on which Apple and Google compete, requiring Google to enact a notarization system which lowers security on Android devices puts Android at a competitive disadvantage relative to iOS.[96]

70. Finally, Epic's proposal would force the Court into micromanaging Android's security paradigm. The Court would need to determine who would be responsible for providing the "generally available, distribution-agnostic notarization-like process" Epic discusses in its Proposed Injunction and would need to answer many questions in implementing this remedy.[97] What standards would such a notarization process need to meet? Will the notarization entity be allowed to charge for its services? How will the price for the notarization process be determined? How will the price be adjusted over time? Will the

---

continuously monitor all of the apps that it has previously reviewed and approved, including apps that are within the Google Play Store and outside of the Google Play Store); 2248:9-17 ("Q. Would decentralized notarization lead to overall lower security than today? …A. Yes…I can talk about two issues here. One, it's what's called race to the bottom…and, two, there is an increased risk of stolen keys when you have multiple reviewing entities.").

94 Kleidermacher Declaration, ¶¶ 23-24 ("a basic notarization system would cost at least tens of millions of dollars per year to operate, and likely over $100 million per year, and even at that level of spending the system would not provide the same degree of safety as the app review process employed by the Play store today. Building such a system would also take a significant amount of time and could not realistically be implemented in a few months…And to the extent that this review process requires human review to provide adequate security assurances, Google would need to employ additional security analysts to review apps distributed outside the Play store.").

95 Trial Testimony of James Williamson Mickens, *In re Google Play Store Antitrust Litigation*, 3:21-md-02981-JD, November 21, 2023 ("Mickens Trial Testimony"), 2175:7-17 ("Q. Right. In your proposal, Google could choose to charge for app review based on an app's size; correct? A. It could. That's a thing that could happen…Q. And, similarly, under your proposal, Google could even charge a developer a percentage of the revenue earned by the app; right? A. That's a thing that could happen from the technical perspective, yes.").

96 Mickens Trial Testimony, 2207:14-25 ("Q. And you were asked whether Apple and Google compete. Do you recall that? A. I do. Q. What do you understand that term to mean in the context of your testimony here? A. So I'm not an economist and so, you know, I can't talk about what competition means in the antitrust sense. My understanding as a security expert and an engineer is that both Apple and Google, they, you know, have engineers they have security people who are working on adding various features to their phone. And so there's sort of like a technical rivalry there, a technical competition.").

97 Epic's Proposed Injunction, II.B.2.ii.

responsible entity be forced to notarize all the apps submitted for notarization, or can it have discretion related to which apps—and apps from which developer—it does and does not notarize? Who will oversee the notarization work and ensure that it meets a minimum quality standard? Who will revise standards and prohibitions as the security landscape rapidly evolves, and will this guidance be subject to regular revision to account for this?

71. Dr. Bernheim contends that all of these provisions are necessary because the States' Settlement (i) fails to restrict Google from "technologically hinder[ing] off-Play distribution channels," (ii) provides latitude with regards to "security and privacy" that is not appropriate, (iii) includes only certain Android versions, and (iv) limits the remedy to four years.[98]

72. With regards to (i), Dr. Bernheim's contention that the States' Settlement does not sufficiently prevent technological hindering of off-Play distribution is based on his stated principle that "warnings should not discriminate among apps based on the app store from which users download them, or discriminate against stores based on whether they are pre-loaded or obtained from the web."[99] Dr. Bernheim presents no economic basis for this principle nor does he address the security, privacy, and user choice issues it raises that I summarize above.

73. With regard to (ii)-(iv), Dr. Bernheim fails to articulate a way to determine the appropriate latitude, scope, or terms of the security provisions. Dr. Bernheim does not explain why it is necessary—or even whether it is feasible[100]—for the remedy to apply to older / deprecated versions of Android, nor does he address whether the benefits would be commensurate with the cost of doing so.

E. Access to Android and Other Google Products or Services (II.C)

74. Under Epic's Proposed Injunction, Google would be prohibited from entering into agreements that deny or impede any "Alternative Android App Distribution Channel" or any Android app downloaded from such a channel from access to functionality or features in Android, Google's proprietary APIs, or Google Mobile Services that is enjoyed by non-

---

98 Bernheim Statement, ¶ 32.

99 Bernheim Statement, ¶ 20. Dr. Bernheim's specific contention is that in terms of "preventing Google from 'imposing frictions on 'off-Play' app installations' … the States' remedy falls short of the Proposed Injunction's requirements concerning parity for off-Play installations, which could allow Google to technologically hinder off-Play distribution channels." Bernheim Statement, ¶ 32.

100 *See* Kleidermacher Declaration, ¶ 41 ("Once a final version of Android has been publicly released, Google does not typically update old versions of Android other than to release critical security patches. This is important because changing the functionality of old versions of Android can cause apps to unexpectedly malfunction if developers did not build their apps to anticipate the new changes. Google also does not have any mechanism to force updates to old versions of Android because OEMs control the availability of updates on their devices.").

Google apps downloaded through Play.[101] Google also would be prohibited from entering into agreements that impede, restrict or condition access to Google's products or services—other than Google Play Billing ("GPB") services—on the basis of a developer's actual or intended use of any "Alternative Android App Distribution Channel."[102]

75. This proposed remedy was not addressed in the States' Settlement.

76. Dr. Bernheim acknowledges that these provisions "go[] beyond prohibiting the conduct the jury deemed illegal at trial," but claims they are designed to "ensure that Google does not undermine the remedy" by limiting apps' access to key Android functionalities or Google products/services based on their distribution channel.[103]

77. These proposed terms would require Google to give developers free access to valuable functionalities and features resulting from Google's investments in developing Android and Play. It would impose this requirement for any functionalities or features that Google makes available to any non-Google apps downloaded through Play. Allowing developers to access all such features and functionalities for free would diminish Google's incentive to continue to invest.[104]

78. For example, Google currently offers two versions of its location services API: (i) an open-source version that is free and available for anyone to use (including non-GMS devices), and (ii) a proprietary closed-source, improved version—only available on GMS devices—that combines on-device signals with Google data to determine device location with more accuracy and less battery drain.[105] Under Epic's Proposed Injunction, Google could be

---

101 *See* Epic's Proposed Injunction, II.C.1.

102 *See* Epic's Proposed Injunction, II.C.2.

103 Bernheim Statement, ¶¶ 58, 60.

104 Pindyck, Robert S., and Daniel L. Rubinfeld, *Microeconomics*, 8th Ed., Pearson, 2013, at p. 693 ("[T]he presence of free riders makes it difficult or impossible for markets to provide goods efficiently."). *See also* Bernheim Amex Trial Testimony, 6427:2-6427:6 ("If there is free-riding on investment, the first party doesn't have the incentive to make the investment to begin with, or has a reduced incentive and makes the investment at a lower level. As a result, possible benefits are lost."); Hubbard, R. Glenn, and Anthony P. O'Brien, *Microeconomics*, 7th Ed., Pearson, 2019, at p. 179 ("Private firms are usually not willing to supply public goods because of free riding."); Mankiw, N. Gregory, *Principles of Economics*, 6th Ed., South-Western Cengage Learning, 2012, at p. 221 ("Profit-seeking firms spend a lot on research trying to develop new products that they can patent and sell, but they do not spend much on basic research. Their incentive, instead, is to free ride on the general knowledge created by others.").

105 Declaration of Kurt Williams in Support of Google's Objections to Proposed Injunction, *In re Google Play Store Antitrust Litigation*, 3:21-md-02981-JD, May 2, 2024 ("Williams Declaration"), ¶ 5 ("Play services includes an API called FusedLocationProvider that makes it easier for developers to determine a user's location in tricky environments, such as dense urban centers where tall buildings interfere with traditional GPS data. To solve this problem, Google has invested in advanced 3D imaging of cities and maps of known WiFi network locations. Google continuously maintains this data, and can then combine it with information from a user's device to determine a more accurate location.");.Van Diggelen, Frank, and Jennifer Wang, "Improving Urban GPS Accuracy for Your App," *Android Developers Blog,* December 7, 2020,

required to make its proprietary version of its location services API available for free on non-GMS devices. Thus, other platforms would be allowed to free ride on Google's investments in GMS devices.

79. Similar to Epic's proposal to share Play's apps with other app stores (which I discuss further below), requiring Google to share all features and functionalities developed for apps in Play will harm competition by preventing Google from engaging in competition on the merits. Other app stores could offer exclusive or differentiated APIs and services to their apps, but Google could not compete by offering exclusive or differentiated features to developers to attract them to and/or retain them on Play.

80. In addition to its adverse economic consequences, this proposed remedy would raise substantial practical issues in implementation. For example, certain APIs offer functionality that relies on an app having been downloaded from Play, such as the SafetyNet API that determines whether an app on the user's device has been modified since it was downloaded from Play.[106] Such APIs would not function with non-Play app stores. Epic's proposal also requires that Google provide access to proprietary, closed-source APIs if an API provides functionality that is "traditionally part of an operating system or platform." It is not clear how Epic intends the Court to determine on an ongoing basis which features or functionalities are traditionally part of an operating system or platform and which may be fairly considered separate. This is especially complicated by the significant degree to which operating systems have evolved over time to provide functionality that was previously provided only by third-party software.[107]

81. Similarly, it is unclear how and in what circumstances Google could charge for access to its APIs. As explained in **Section II**, regulating these prices or preventing Google from earning a return on its investments in developing APIs could harm consumers.

F. Catalog Access and Library Porting (II.D.1)

82. Under Epic's Proposed Injunction, for a period of 6 years, Google would be required to (i) provide third-party app stores access to Play's app catalog via an API that allows all Play apps to be viewable in the third-party app store and fulfills download requests made

---

https://android-developers.googleblog.com/2020/12/improving-urban-gps-accuracy-for-your.html, accessed April 23, 2024 ("the latest improvements to the Fused Location Provider API…improve[] battery life.").

106 Williams Declaration, ¶ 8. *See also*, Williams Declaration ¶ 9 for an example of an API that relies upon the user having a Google account, which may not be required by other app stores.

107 As an early example of this trend, prior to 2013 the ability to turn on/off the iPhone camera flash for use as a flashlight was only provided by third-party apps. In 2013, this functionality became part of iOS 7. Gallagher, William, "Flashlight on iPhone – Everything You Needs to Know," *AppleInsider*, January 15, 2021, https://appleinsider.com/articles/21/01/15/flashlight-on-iphone---everything-you-need-to-know, accessed April 30, 2024.

by users of the third-party store ("catalog access");[108] and (ii) provide users with the ability to share a list of apps installed by Play on a user's device and provide users the ability to change ownership of those apps to a third-party app store, subject to a one-time user permission ("library porting").[109] Once ownership for an app has been transferred, the third-party app store will obtain the subsequent service fee revenue associated with that app.[110]

83. Epic's experts did not argue at trial that it is anticompetitive for Google not to provide catalog access and library porting. These proposed remedies were not part of the States' Settlement.

84. Dr. Bernheim contends that catalog access "provides rival app stores with immediate scale on the developer side, allowing them to compete for users on the merits without confronting a chicken-and-egg problem." He claims this will in some manner encourage rival app stores to develop relationships with OEMs, and attract developers to the app store "as it builds its user base."[111] With respect to library porting, Dr. Bernheim states that rival app stores can "choose to incentivize" developers to port update privileges to the rival app store and the "resulting competition between Google Play and its rivals will directly benefit users."[112] He acknowledges that "this provision goes beyond prohibiting the specific conduct, or substantially similar conduct, that was at issue in the trial, in order to counter the persistent impact of Google's past anticompetitive conduct."[113]

85. In **Section II** above, I discuss why I believe these claims are incorrect as a matter of economic principle, and why I disagree that it is necessary to actively restructure the market in order "reestablish an even playing field." I note that Dr. Bernheim has testified that "the best strategy for overcoming network externalities is to offer distinctive content not available on the Google Play Store,"[114] and that Epic itself has argued that it successfully used this strategy to enter and compete with Steam and other established game distributors on PCs.[115] In this section, I focus on the details of the proposed catalog access and library porting remedies.

---

108 *See* Epic's Proposed Injunction, II.D.1.i.

109 *See* Epic's Proposed Injunction, II.D.1.ii.

110 *See* Epic's Proposed Injunction, II.D.1.

111 Bernheim Statement, ¶¶ 63-64.

112 Bernheim Statement, ¶ 64.

113 Bernheim Statement, ¶ 68.

114 Bernheim Statement, ¶ 48. *See also* Bernheim Statement, ¶ 13.

115 Allison Trial Testimony, 230:17-233:9 ("Q… Did Epic use any other strategies to grow the store? A… it was really important for us to get important games and strategic partnerships that players would be excited about exclusively for a timed exclusive period… consoles have used timed exclusives as a business strategy to

86. From an economic point of view, catalog access is not necessary for competition because third-party app stores are already free to compete to offer any app that is offered in Play. Third-party app stores can compete to attract Android app developers by offering a high-quality app store at an attractive price. Developers benefit from this competition among app stores.

87. The proposed catalog access and library porting remedies would threaten these benefits because they would allow third-party app stores to obtain access to millions of apps without having to offer the developers of those apps more value. Developers that are not offered those deals will be harmed by this lack of competition. Fewer incentives and less co-investment offered to developers could degrade the overall quality of apps. Although competing app stores may still have incentives to attract certain developers of high-revenue apps in order to capture service fee revenue, these incentives will not extend to the large number of free and low-revenue apps that constitute the vast majority of apps that would be covered by catalog access and library porting. These apps collectively provide substantial value to users, and under the proposed remedy, competing app stores would have weakened incentives to attract the developers of these apps.

88. Developers would suffer further harm from losing control over the distribution of their apps. A developer that agrees to put its apps on Play may not want to have its apps appear on a potentially less reputable storefront (e.g., next to gambling or pornography apps), or in a store that provides a lower-quality experience for users. For example, GetJar, an alternative app store, lists several suspicious apps that contain hacking tools such as "WhatsApp Hack Tool" or "PUBG Mobile Hack" alongside seemingly reputable apps.[116] Another app store, APKPure, states that all its APK files are the same as the ones on Play, but the app store allows users to download older app versions that can compromise privacy

---

grow their platforms as well for decades, and we had never seen that in PC. So we also decided to pursue a very similar strategy."); Dingman, Hayden, "A Year in, the Epic Games Store's Fight Against Steam has Made PC Gaming Better For Everyone," *PCWorld,* December 6, 2019, https://www.pcworld.com/article/398473/a-year-in-the-epic-games-stores-fight-against-steam-has-made-all-pc-gaming-better.html, accessed April 21, 2024 ("In 2019 … Epic shelled out a ton of money for timed exclusives. Good ones, too!"); Statt, Nick, "Epic vs. Steam: the Console War Reimagined on the PC," *The Verge,* April 16, 2019, https://www.theverge.com/2019/4/16/18334865/epic-games-store-versus-steam-valve-pc-gaming-console-war-reimagined, accessed April 21, 2024 ("Sweeney says the company will continue this strategy [of securing exclusive titles for its store], either until Epic's store becomes popular enough to stand on its own or Valve acquiesces to more developer-friendly terms.").

116 Christian Cawley, "Avoid GetJar! Thousands of Free Mobile Apps With the Risk of Malware," *MakeUseOf*, February 18, 2020, https://www.makeuseof.com/tag/getjar-thousands-free-apps-mobile-phone/, accessed April 10, 2024 ("it's home to plenty of unpopular, out of date, and downright suspicious apps, too… GetJar isn't as reliable as the Play Store or other alternatives because of the following issues: Apps are of unreliable origin[;] GetJar lists hacking tools[;] … Risk of malware and ransomware[;] For every Facebook Lite, there's a 'WhatsApp Hack Tool' or a 'PUBG Mobile Hack.' … Google Play is a safe, trusted library of software for your mobile device. GetJar is not."). The GetJar app store also includes apps with lewd or profane content. *See, e.g.,* "Find the Best Banned APK Mobile Android Apps and Games Below," *GetJar*, https://www.getjar.com/tag/Banned/, accessed April 10, 2024.

and security.[117] Some app stores permit apps with adult content.[118] Under the proposed remedy, a developer's app could potentially appear in these or other storefronts without the developer's knowledge or consent. If developers lose control of their apps on Android and cannot have a say on where they appear, that may lead them to deprioritize investments in Android, to the benefit of Apple. Moreover, when agreeing to the DDA, developers select the countries where their apps should be distributed, and could face regulatory issues (e.g., tax compliance) if their apps are distributed elsewhere by third-party app stores.[119] An app developer may prefer to limit access to its apps to protect its reputation, and to avoid the cost of managing multiple distribution channels.

89. Reduced competition would also harm users. App stores would have weakened incentives to offer better prices, quality, and features for users because they would not need to attract more users in order to attract more developers.

90. Finally, the proposed catalog access remedy would enable a textbook example of free riding: competing app stores could effectively offer clones of Google's own catalog rather

---

117 Joshua, Crissy, "A Guide to APKPure: Is It Legal and Is It Safe?," *Avast*, September 22, 2023, https://www.avast.com/c-is-apkpure-safe, accessed April 10, 2024 ("Downloading older versions that are available on APKPure can be risky because older app versions can have outdated defense mechanisms against online threats, or specific vulnerabilities in their code that could allow hackers access to your phone… anyone can download age-restricted apps on APKPure.…Some age-restricted apps also come equipped with online tracking to target users with specific ads that aren't appropriate for children."); "About Us," *APKPure*, https://apkpure.com/about.html, accessed April 10, 2024. Additionally, while APKPure claims that its apps have been scanned by Google and are completely safe, APKPure was infected with a trojan malware in 2021 that could show ads on users' devices, collect device information, and download other malware. Golovin, Igor, "Infected Android App Store," *Kaspersky*, April 9, 2021, https://www.kaspersky.com/blog/infected-apkpure/39273/, accessed April 10, 2024.

118 Trial Testimony of Steven Allison, *In Epic Games, Inc. v. Apple Inc.,* 4:20-cv-05640*,* May 7, 2021 ("Allison Apple Trial Testimony"), 1257:18-1258:7 ("Q. … There are many games on Itch.io. I won't even read the names out loud. A. Okay. Q. But they are both offensive and sexualized. You're not aware of that? A. Itch.io is an app store that is not the Epic Games Store. We are not distributing -- Itch is distributing Itch.io's games. Epic is only distributing the app store Itch.io. Q. And Itch.io is now available as an app on the Epic Games Store; correct? A. Correct. Q. And those apps in Itch.io have not gone through any review process whatsoever; correct? A. They are subject to whatever process Itch.io puts in front of their developers.").

119 For example, in certain countries, taxes must be included in the price shown to consumers who wish to make in-app purchases, but that is not the case in other countries. These differences in taxation laws could lead to tax compliance issues for developers if their apps are copied without their consent to third-party app stores used in other jurisdictions with different taxation regulation. "Tax Rates and Value-Added Tax (VAT)," *Play Console Help*, https://support.google.com/googleplay/android-developer/answer/138000?hl=en&ref_topic=3452890&sjid=14852023290812909701-NA, accessed April 10, 2024 ("In some countries, prices shown to buyers on search and detail pages must equal the amount paid at the time of payment. This means that all taxes (including VAT) must be included in the price."). *See also* "Requirements for Distributing Apps in Specific Countries/Regions," *Play Console Help*, https://support.google.com/googleplay/android-developer/answer/6223646?hl=en, accessed April 10, 2024, which explains country-specific information related to distribution (e.g., developers distributing apps in Japan must notify the Japanese authorities if they are to deliver a game that will be billed in Japan in accordance with the Payments Services Act in that country: "you are required to comply with all applicable laws in Japan (for example, the Payment Services Act) when distributing apps in Japan.").

than investing or competing to develop their own.[120] A competing app store could offer its consumers the full catalog of Play apps (3.33 million apps as of April 2024),[121] benefitting from Play's security screening and verification, Play's download and update functionality, Play's developer relationships, and other Play features and functions.

91. Although Google would continue to obtain service fee revenue from some of these apps, it would be providing its competitors with the benefits of being able to offer the apps to users and guarantee them a comprehensive, high-quality catalog without receiving any compensation from those competitors in return. Moreover, it would receive no revenue from the vast majority of apps that would be shared through catalog access because those apps do not monetize through download fees or in-app purchases. Finally, as discussed below, it would lose all revenue from apps shared through this remedy when ownership of them is changed through library porting.

92. The proposed remedy would be analogous to requiring Walmart to allow other local retailers to offer their customers any product that Walmart stocks, offering those retailers full access to Walmart's internal supply-chain data, and requiring Walmart to process and ship any orders consumers place for Walmart products at Walmart's competitors. As discussed in **Section II**, free riding of this kind undermines competitive markets because it reduces the incentives of all market participants to invest and innovate.

93. Implementation of the proposed catalog remedy in a way that addresses privacy and security issues as well as developers' lack of control is challenging. What technical conditions would the catalog access mechanism that Google would provide need to satisfy? How much control will developers have over where their apps appear? What recourse will app stores have if they are unsatisfied with this mechanism or if they encounter technical problems? What standards will Google be able to impose on third-party app stores that wish to display its catalog listings and use its brand name? What steps will Google be allowed to take to protect users' security? If the conditions that Google can set in its agreements with competing app stores are determined by the Court, how will these agreements be monitored? How will these conditions evolve in the face of changing technology?

94. The library porting provision of Epic's proposed remedy would allow users to provide any third-party app store a full list of apps installed by Play on a user's device and allow these app stores to take control of updating these apps subject only to a single, one-time permission from the user, provided that the apps are listed on that app store. The proposed remedy does not envision Google having the ability to impose any limitations on which

---

120 *See, e.g.,* Mankiw, N. Gregory, *Principles of Economics*, 6th Ed., South-Western Cengage Learning, 2012, at p. 220 ("free rider[:] a person who receives the benefit of a good but avoids paying for it.").

121 "Google Play vs the Apple App Store: App Stats and Trends," *42matters*, April 9, 2024, https://42matters.com/stats, accessed April 10, 2024.

stores it would share this user information with, nor does it specify what if any conditions Google may impose on library porting or how visible or reversible the decision to switch app stores would be to a user. This could harm users in at least three ways.

95. First, library porting would risk undermining the security and functionality of apps, for example through reduced updating. Developers update their apps for many reasons, including to address potential security issues or fix bugs. If some apps originally downloaded from Play—and taken over by other app stores as a result of the library porting provision—are not updated as regularly as they would be on Play, then their security and functionality will be compromised.

96. Second, library porting would risk substantial confusion for users by making it difficult to determine which apps are being controlled or updated by which stores. A user of an app who wishes to check for updates, diagnose a problem, or understand unexpected behavior may be confused or frustrated if they cannot determine which store is in control.

97. Third, sharing information on the catalog of apps installed on a device with all app stores would undermine user privacy. For example, such a list could reveal information to an app store about a user's health or sexual orientation, and that information might in turn be shared to other third parties without the user's consent. While users anticipate that this information in the set of apps they download is visible to Google, they may not recognize that it is also visible to any third-party app store they choose to download and install.

98. Library porting would also enable egregious free riding. Epic's proposal transfers service revenue to third-party app stores that have taken over app update privileges: a store that entices a user to port a set of apps would capture the full revenue stream from those apps even though the user's discovery, evaluation, and download of the apps relied on a higher-quality store. Third-party stores might seek to gain control of the highest-revenue apps users had discovered through Play, while leaving Google to pay the cost of maintaining and updating free or low-revenue apps. This kind of free riding would not only produce the usual harms such as reduced investment and innovation, but it would give app stores enormous incentives to convince users to click a button that would hand over the app store ownership of their most lucrative apps, and could lead to a barrage of pop-ups, notifications, and offers, including many that might be highly deceptive. Stores would compete to capture the revenue from apps downloaded from Play rather than competing to offer users and developers a higher quality store of their own. That would harm users by degrading their experience.

99. As with the catalog access proposal, the library porting proposal also raises many questions in implementation: What information would be provided by a third-party app store to the user, when the user is asked to choose whether the ownership of their Play-downloaded app could be taken over by the third-party app store? If the user accepts a change of ownership, will they be able to switch back to Play at a later date? If so, when and how can Play prompt them to do so? If developers opt to delist from third-party app

stores can ownership of the app be passed back to Play or would users be forced to re-install the apps? The Court would also need to answer questions regarding any mechanism for developers to choose whether the ownership of their apps could be changed, including any recourse they may have if they are unsatisfied with the treatment of their apps by the third-party app store.

G. Distribution of Third-Party App Stores on Play (II.D.2)

100. Under Epic's Proposed Injunction, for a period of 6 years, Google would be required to allow distribution of competing third-party app stores on Play.[122]

101. This proposed remedy does not address any conduct challenged or identified as anticompetitive by Epic's experts at trial, and as recognized by Dr. Bernheim "the Court ruled that Google [is] not obligated as a matter of antitrust law to carry other app stores on Google Play."[123] This proposed remedy was not directly addressed in the States' Settlement, although provisions in the States' Settlement promote the preinstallation and distribution of third-party app stores outside Play.[124]

102. Dr. Bernheim states that "this provision goes beyond prohibiting the specific conduct, or substantially similar conduct, that was at issue in the trial, in order to counter the persistent impact of Google's past anticompetitive conduct"[125] Dr. Bernheim claims that this provision is necessary given that "[i]f third-party app stores were not available through Google Play, many users would not know where to find them or even to look for them at all" which will assist in competition for users.[126]

103. This proposed remedy would harm consumers in several ways. First, it carries substantial security risks for users. Academic research indicates that alternative app stores can be a significant vector of malware.[127] Play provides value to users in part by providing an assurance that an app downloaded through Play has been screened for security. Such

---

122 *See* Epic's Proposed Injunction, II.D.2.

123 Bernheim Statement, ¶ 68.

124 *See* States' Settlement, §§ 6.6, 6.7, 6.8, 6.9.1, and 6.9.2.

125 Bernheim Statement, ¶ 68.

126 Bernheim Statement, ¶ 67.

127 *See, e.g.,* Kotzias, Platon, *et al.*, "How Did That Get In My Phone? Unwanted App Distribution on Android Devices," *2021 IEEE Symposium on Security and Privacy*, 2021, pp. 53-69, at p. 62 ("We observe significant differences in [installer detection ratio (IDR), i.e., the fraction of unwanted APKs installed over the total number of APKs installed] for different markets. The highest IDR of 11.7% is for the Huawei … followed by the Iranian Bazaar market … with 10.5%, the Iranian MyKet market … with 4.4%, the NearMe market from Chinese vendor Oppo … with 2.8%, and the 9Apps Indian market … with 1.6% IDR. On the better side of the spectrum, there are the Play market and Amazon's market with the lowest IDRs of 0.6% and 0.7% respectively.").

screening is likely to become less effective or trustworthy if an app can download, install, and modify additional software that has not gone through this screening process. Dr. Qian explained at trial that it would be difficult for Google to assess the security risks associated with apps that a particular app store might at some point make available because any process will inherently be reactive as Google does not have immediate access to apps from alternative app stores.[128]

104. Second, under the proposed remedy, Google could be forced to distribute app stores that in turn distribute content (e.g., pornography) that violate Google's content restrictions. During the *Epic v. Apple* trial, it was revealed that the itch.io app store distributed through the Epic Games Store contains adult content which the Epic Games Store is not responsible for reviewing.[129] Another example is Tencent MyApp where users can download third-party app stores such as 360 Mobile Assistant, Baidu Mobile Assistant, and Wandoujia.[130] The latter two distributed Bilibili, a video-sharing website, which was removed by Chinese authorities in 2018 for hosting explicit and inappropriate content.[131] Baidu Mobile Assistant also had a fake CCleaner app that exposed users to adware.[132]

---

128 Qian Trial Testimony, 2245:16-2246:1 ("if Google has previously approved an app, generated a token for that app, it doesn't mean that app is going to be safe forever. … so in order to mitigate that risk, Google would have to continuously monitor all of the apps that it has previously reviewed and approved, including apps that are within the Google Play Store and outside of the Google Play Store.").

129 Allison Apple Trial Testimony, 1257:18 – 1258:7 ("Q. … There are many games on Itch.io. I won't even read the names out loud. A. Okay. Q. But they are both offensive and sexualized. You're not aware of that? A. Itch.io is an app store that is not the Epic Games Store. We are not distributing -- Itch is distributing Itch.io's games. Epic is only distributing the app store Itch.io. Q. And Itch.io is now available as an app on the Epic Games Store; correct? A. Correct. Q. And those apps in Itch.io have not gone through any review process whatsoever; correct? A. They are subject to whatever process Itch.io puts in front of their developers.").

130 "Baidu Mobile Assistant," *Tencent*, https://sj.qq.com/appdetail/com.baidu.appsearch, accessed April 10, 2024 (the source was translated from its original language using Google Translate); "Wandoujia," *Tencent*, https://sj.qq.com/appdetail/com.wandoujia.phoenix2, accessed April 10, 2024 (the source was translated from its original language using Google Translate); "Qihoo 360," *Tencent*, https://sj.qq.com/appdetail/com.qihoo.appstore, accessed April 10, 2024 (the source was translated from its original language using Google Translate).

131 "Bilibili," *Wandoujia*, https://www.wandoujia.com/apps/281291, accessed April 10, 2024, https://www.wandoujia.com/apps/281291 (the source was translated from its original language using Google Translate); "Bilibili," *Baidu Mobile Assistant*, https://shouji.baidu.com/detail/3975824193, accessed April 10, 2024 (the source was translated from its original language using Google Translate); Yujie, Xue, "Bilibili Removed From Android App Stores for Promoting Incest," *Sixth Tone*, July 27, 2018, https://www.sixthtone.com/news/1002698, accessed April 10, 2024 ("Bilibili, an anime-centered video platform especially popular with millennials, has been removed from several app stores in China after it was criticized for inappropriate content.").

132 "Fake Mobile CCleaner App Sneaked into the China Baidu App Store," *Decoded Avast.io*, March 4, 2019, https://decoded.avast.io/threatintel/fake-mobile-ccleaner-app-sneaked-into-the-china-baidu-app-store/, accessed April 10, 2024 ("fake mobile CCleaner app has been published in the China Baidu App Store … it's specified as ***Certified Official Version*** … The fake CCleaner app uses the good brand reputation of the

105. Third, requiring Google to distribute third-party app stores would reduce the returns OEMs could earn from preinstallation deals, and this could in turn lead OEMs to increase device prices to users. App stores compete for preinstallation by offering payments to OEMs and by improving the quality of the app stores, which makes them more attractive to OEMs to preinstall. Under Epic's proposed remedy, third-party app stores would have substantially reduced incentives to offer OEMs monetary or other incentives for preinstallation. If app stores can get installation through Play, they would have less reason to pay OEMs for preinstallation.

106. Fourth, like the catalog access and library porting remedies, requiring Google to distribute third-party app stores would force Google to subsidize its rivals, creating another textbook example of free riding.[133] It would be analogous to requiring Walmart to allow kiosks promoting Target within its stores or requiring Airbnb to promote the competing site VRBO on its website. Google has made and continues to make enormous investments in Play, to the benefit of consumers. If those investments will benefit competitors, then Google will have less incentive to make them. Rival app stores will also have less incentive to invest, as they can free ride on distribution through Play rather than competing to secure distribution themselves.

107. The fact that virtually all third-party app stores, including the Samsung Galaxy Store and Amazon Appstore, prohibit the distribution of competing app stores within their stores provides evidence of these potential harms.[134] Like Play, these app stores are incentivized

---

genuine CCleaner app 4.11.1 and repackages it to include adware in order to aggressively monetize mainland China users." Emphasis in original.).

133 *See, e.g.,* Mankiw, N. Gregory, *Principles of Economics*, 6th Ed., South-Western Cengage Learning, 2012, at p. 220 ("free rider[:] a person who receives the benefit of a good but avoids paying for it."). *See also* Pindyck, Robert S., and Daniel L. Rubinfeld, *Microeconomics*, 8th Ed., Pearson, 2013, at p. 693 ("free rider[:] Consumer or producer who does not pay for a nonexclusive good in the expectation that others will.").

134 *See, e.g.*, "App Review Guidelines," *Apple Developer App Review*, April 5, 2024, https://developer.apple.com/app-store/review/guidelines/, accessed April 10, 2024 ("Unacceptable[:] [c]reating an interface for displaying third-party apps, extensions, or plug-ins similar to the App Store or as a general-interest collection."); "Monetization and Advertising Policy" *Amazon Developer Policy Center*, October 16, 2023, https://developer.amazon.com/docs/policy-center/monetization.html, accessed April 10, 2024 ("app scenarios that violate the Amazon Appstore Content Policies[:]…[a]n app that is actually a separate app store from the Amazon Appstore."); "App Distribution Guide," *Samsung Developer*, https://developer.samsung.com/galaxy-store/distribution-guide.html, accessed April 10, 2024 ("Apps must not support the download of any other app by a direct method from inside the app (for example, through an APK)."); "Aptoide Publisher Distribution Agreement," *Aptoide*, November, 2020, https://en.aptoide.com/company/legal?section=distribution, accessed April 10, 2024 ("You may not use the Aptoide App Store to distribute or make available any App whose primary purpose is to facilitate the distribution of software applications and games for use on Android devices outside of the Aptoide App Store."); "Review Guidelines," *Xiaomi Developer*, https://global.developer.mi.com/document?doc=appReview.reviewGuidelines, accessed April 10, 2024 ("Apps that have AppStore function (e.g. app search, download or update) will be rejected."); "App Content," *Huawei Developers*, August 23, 2023, https://developer.huawei.com/consumer/en/doc/app/50104-04, accessed April 10, 2024 ("Your app must not be an app distribution platform, including but not limited to an app market or a game center."); "App Review

to compete by investing in their stores and protecting the return on such investments by restricting distribution of third-party app stores in their own stores. Among app stores more broadly (not just on mobile), the only one I am aware of that has allowed the distribution of third-party app stores is the Epic Games Store on Macs and PCs that, as highlighted above, has historically distributed apps like itch.io, which contains adult content that the Epic Games Store does not review.[135]

108. Dr. Bernheim acknowledges that "there are good reasons to be cautious about requiring the Google Play Store to carry competing stores in perpetuity."[136] I agree. However, these same "reasons" also suggest caution in requiring Play to carry competing stores for a period of six years, which is a long period given the rapidly changing technological landscape. Dr. Bernheim's only rationale for the six-year term is that it corresponds to roughly two purchase cycles for a typical phone user. This fact does not establish that the harms of the remedy—which Dr. Bernheim acknowledges are large enough to imply caution over a longer time horizon—would not outweigh any alleged benefits over a period of six years.

109. Further, requiring Google to distribute third-party app stores through Play would raise a series of issues that the Court would need to resolve in order to reduce harms to OEMs, carriers, users, developers, and Google itself (that cannot be fully eliminated).

110. First, the economic principles discussed in **Section II** dictate that it would be essential for Google to be able to charge a service fee for any distribution it provides to third-party app stores through Play, just as it currently can charge for distribution of apps and other services. This could include fees on in-app purchases within apps downloaded from these stores and/or fees proportional to the stores' total revenues. Such fees would not eliminate the incentive to free ride and thus would not eliminate the harms to OEMs, carriers, users, and developers from this remedy, but they would mitigate the harms to some degree. Requiring Google to give away its distribution and discovery services for free would further diminish third-party app stores' incentives to pay OEMs for preinstallation, magnifying harms to users and ultimately developers, and would further reduce Google's

---

Standards," *OPPO Developer*, https://developers.oppomobile.com/wiki/index#id=17, accessed April 10, 2024 ("Prohibited app behaviors[:]… The main function of the app is market- oriented (allowed to be downloaded, updated and searched). … The full page provides a large number of third-party apps for download."); "Guidelines for App Verification on the Developers Platform," *Vivo Developers*, https://developer.vivo.com/doc/detail?id=25, accessed April 10, 2024 ("Apps are excluded under the following circumstances: … The app is a product for distribution: (1) The app itself is a distribution app."); "Privacy Policy Submission Content and Review Specifications," *Tencent Open Platform*, https://wikinew.open.qq.com/#/iwiki/875339652, accessed April 10, 2024 (the source was translated from its original language using Google Translate).

135 "Itch.io," *Epic Games Store*, https://store.epicgames.com/en-US/p/itch-io, accessed April 10, 2024 ("itch.io is an open marketplace for independent digital creators with a focus on independent video games[.]").

136 Bernheim Statement, ¶ 26.

EXHIBIT J

Brian C. Rocca, S.B. #221576
brian.rocca@morganlewis.com
Sujal J. Shah, S.B. #215230
sujal.shah@morganlewis.com
Michelle Park Chiu, S.B. #248421
michelle.chiu@morganlewis.com
Minna Lo Naranjo, S.B. #259005
minna.naranjo@morganlewis.com
Rishi P. Satia, S.B. #301958
rishi.satia@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105-1596
Telephone: (415) 442-1000

Neal Kumar Katyal, *pro hac vice*
neal.katyal@hoganlovells.com
Jessica L. Ellsworth, *pro hac vice*
jessica.ellsworth@hoganlovells.com
HOGAN LOVELLS US LLP
555 13th St. NW
Washington, D.C. 20001
Telephone: (202) 637-5600

Counsel for Defendants

Glenn D. Pomerantz, S.B. #112503
glenn.pomerantz@mto.com
Kuruvilla Olasa, S.B. #281509
kuruvilla.olasa@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, CA 90071
Telephone: (213) 683-9100

Justin P. Raphael, S.B. #292380
justin.raphael@mto.com
Dane P. Shikman, S.B. #313656
dane.shikman@mto.com
Rebecca L. Sciarrino, S.B. #336729
rebecca.sciarrino@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty Seventh Floor
San Francisco, CA 94105
Telephone: (415) 512-4000

Jonathan I. Kravis, *pro hac vice*
jonathan.kravis@mto.com
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Ave. NW, Suite 500E
Washington, D.C. 20001
Telephone: (202) 220-1100

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION THIS DOCUMENT RELATES TO: *Epic Games Inc. v. Google LLC et al.*, Case No. 3:20-cv-05671-JD	Case No. 3:21-md-02981-JD **GOOGLE'S PROFFER REGARDING EPIC'S PROPOSED REMEDIES** Judge: Hon. James Donato **PUBLIC REDACTED VERSION**

TABLE OF CONTENTS

Page

I. INTRODUCTION

At the Court's direction, ECF No. 978, Google respectfully submits this proffer describing the technical work and estimated costs to: (i) provide third-party app stores with access to Google Play's app catalog; (ii) provide "library porting" of users' Play-installed apps to third-party app stores; and (iii) distribute third-party app stores through the Google Play store. Accompanying this proffer are the declarations of four senior Google employees: (1) Vitor Baccetti (Group Product Manager), (2) Edward Cunningham (Director of Product Management), (3) David Kleidermacher (Vice President of Engineering for Security and Privacy for Android and Made-by-Google Products and Services), and (4) Christian Cramer (Finance Director for Android Ecosystem).

In submitting this proffer, Google does not waive and maintains its objections to Epic's proposed injunction, *see* ECF No. 958. Google's description of how it would attempt to implement catalog access, library porting, and/or Play distribution of third-party stores, if ordered by the Court, does not reflect any agreement by Google that these remedies, as described in Epic's proposed injunction, are reasonable, appropriate under the law, or feasible absent significant expense and fundamental changes to the way Play and Android operate.

As discussed below, these proposed remedies would require a dramatic redesign of the Play store and Android that would harm Android users and developers, the trust and safety of the Play store, and the Android ecosystem and require Google to become a forced dealer for its competitors. Catalog access would fundamentally change Play's relationship with developers, and would require the design and implementation of a new system to provide developers with information about the options available to them under this new program on a regular basis. It would also require the design and implementation of a new method to provide metadata on Google's catalog to third-party app stores, and additional installation and update services for apps discovered in third-party app stores. Library porting, as described in Epic's proposed injunction, would require changing the Android operating system in ways that would compromise the security of Android users. Distribution of third-party app stores would effectively require Google to build a team to screen third-party app stores for malware, pirated apps, and other content that violates

Play store policies on an ongoing basis. This remedy would also require fundamental alterations to the Play store to transform it from an app store that distributes only apps to an app store that also distributes other app stores—a change that would inevitably harm users, developers, and the Play store brand. It would also require changes to fundamental user security protections in the Android operating system.

These remedies would be very costly and would take a substantial amount of technical work and time to implement. Google's best assessment at this point in time is:

- Catalog access would require 12-16 months to implement, and would cost Google between $27.5 million and $66.9 million to build, implement, and maintain for the duration of the injunction.
- Library porting, as described in Epic's proposed injunction, would require a year to implement, and would cost Google between $1.7 million and $2.4 million to build, implement, and maintain.
- Distribution of third-party app stores would take 12-16 months to implement. This remedy would cost Google between $32.1 million and $67.7 million to build, implement, and maintain for the duration of the injunction, with an additional annual ongoing cost for review of apps and updates in third-party app stores. The cost of this ongoing review depends on the number of third-party app stores that request distribution through Play and the size of their catalogs. Assuming the catalogs of those app stores led to a 20 percent increase in the current review work performed by Play, that cost would be approximately [redacted] per year. For an injunction of two to six years in duration, that additional cost would be between [redacted] and [redacted]

These estimates reflect the technical and review costs to Google. They do not include the incalculable costs that Google would suffer from the harms to the Google and Play brands or to the security and viability of the Android ecosystem caused by these proposed remedies.

This proffer reflects Google's current analysis within the timeframe provided and based on the limited description of the proposed remedies set forth in Epic's proposed injunction. Google

reserves the right to modify this description in response to any further submission by Epic describing these proposed remedies in more detail. Should the Court order Google to implement one or more of these remedies, it is possible that, in the course of complying with that order, Google could encounter unanticipated consequences of the Court's order. That may require Google to pursue different methods of implementation (which may involve different timelines), and Google reserves its right to do so.

Finally, in submitting this proffer, Google renews its request for the opportunity to submit further briefing. In addition to implementation and cost issues, the technical details of Epic's novel proposals raise significant legal issues, particularly in light of the fact that Epic asks this Court to impose a worldwide injunction. Google respectfully requests the opportunity to brief those issues before the Court issues any injunction in this matter.

II. CATALOG ACCESS

Epic's proposed injunction would require Google, for a specified period of time, to provide third-party app stores—Google's competitors—with "access [to] the Google Play Store's catalog of apps not then available on those" stores. ECF No. 952, Proposed Injunction § II.D.1. If a user "wishes to download and install an app not then available on that" third-party store, Google would be required to "have the Google Play Store download and install that app on the Third-Party App Store User's device." *Id.* Epic's injunction effectively asks the Court to override the developers' decision on where to distribute their own apps (which are the developers' intellectual property) and force Google to distribute each developer's apps on stores with which the developer has no relationship and without the developer's express consent. The proposal further allows third-party app stores to free ride on Google's substantial investment in building its catalog, by focusing on building relationships with developers of profitable apps while getting free apps from Google.

If Google were ordered to implement this remedy over its objection, Google currently expects that it would do so in four steps: (1) build, launch, and maintain a method for delivery of the metadata associated with the apps in the Play store catalog, as well as a method for installation of apps through the Play store; (2) create a developer consent mechanism to allow developers to decide whether to participate in catalog access and further share its intellectual property, and if so

in which third-party app stores; (3) develop and implement a model for charging third-party app stores for the service of catalog access and value of Play's catalog; and (4) develop and implement eligibility criteria for third-party app stores that wish to participate in catalog access to mitigate harm to users and developers.

A. App Catalog Metadata Export

Epic's proposed injunction does not describe how Google should provide third-party app stores with "access" to the Play store's catalog or what "access" would constitute in this context. Google assumes that such "access" involves some technological ability for a third-party app store to obtain a listing of the apps available in the Play store.

Google proposes to provide such access through the metadata export process discussed in the Declaration of Vitor Baccetti. *See* Baccetti Decl. ¶¶ 7-10. Specifically, Google would export "metadata" (information about an app, such as the app's name, the developer name, image of the app icon, and app category) associated with the generally available apps in its catalog through a server capable of providing that metadata to any authorized third-party app store's serving system.[1] As discussed below, access to this metadata would be subject to terms of service set by Google. Google would regularly export and refresh this metadata. The third-party store would be able to maintain its own local database containing the exported data, as well as a local database of apps published directly in its store. When displaying apps to a user, the third-party store could query both databases and merge the results to create a single user-facing catalog in the third party's storefront. This process would satisfy Epic's proposal that Google provide third-party app stores with "access" to the "Google Play Store's catalog of apps not then available on those" stores, as Google understands this requirement. ECF No. 952, Proposed Injunction § II.D.1.i.

As Mr. Baccetti explains in his declaration, if the user selects an app published directly in the third-party app store, the store would use its own code to download and install the requested app and Google would not be involved. Baccetti Decl. ¶ 11. If the user selects an app that is

[1] The export would not include metadata for apps that are not publicly available, such as apps that are published only for users in a specific domain (e.g., enterprise-specific apps) or apps in closed beta.

published by Play, but not by the third-party app store, then the third-party store could request that the Play store install the app and deliver the download. This request would be made through an Application Programming Interface ("API") that Google would provide. The API would then render a Google-generated user interface that allows the user to download the app without leaving the third-party app store.[2] (If the user is not eligible to install the app—for example because the user is a minor or because the app is not available in the user's country or is not compatible with the user's device—then the Google-generated user interface would inform the user of this fact.) This interface would contain Play branding, so that the user is on notice that they are downloading an app from the Play store (rather than the third-party store) and that they are signed into a Play account and are agreeing to Play's terms and conditions, just as if they were installing an app directly from the Play store itself. In addition, certain jurisdictions have regulatory requirements regarding the information displayed to users at the point of install, and because Play is fulfilling the installation, Google must be able to generate the interface so it can ensure compliance with those regulations. This process addresses Epic's proposal that such installation be accomplished through "a background process similar to the Alley Oop integration offered by Google to certain third-party Developers," as Google understands that term. ECF No. 952, Proposed Injunction § II.D.1.i .

Because the Play store is handling the installation (and subsequent updates) of the app, the user is treated in the same way as a user who installs an app directly from the Play store. Baccetti Decl. ¶ 18. This means, for example, that the user will be required to agree to relevant Play terms of service (if they have not already done so) and will receive Play points for the installation (if enrolled), and the Play store will, as with any Play user, communicate with the user about updates as well as notifications about Play store products and promotions. The user will also be required to sign into the Play store to complete the installation, and if the user has not previously signed

[2] Google will also need to build and implement an additional security layer that ensures that the app store seeking to call the Play API is, in fact, an app store that the developer has authorized to make the app available through catalog access. This mechanism would involve building and maintaining, in real time, a list of approved callers of the Play API described above. Baccetti Decl. ¶ 16.

into the Play store, then the user will be redirected to the Play store to register. These steps are necessary because the Play store has no mechanism to install apps for a user that is not signed into the store.

The metadata provided to the third-party app store will include fundamental identifiers for the apps in Google's catalog, such as the name of the app, the associated package name, and the name of the developer. Baccetti Decl. ¶ 8. The provided metadata will also include some basic information *provided by the developer* to Google about the app, such as the countries in which the app may be distributed and whether the app offers in-app purchases. The purpose of providing this additional data is to allow the third-party app store to reduce the number of instances in which a user clicks on an app in the third-party app store that the user is not eligible to download, for example because the app is not available in the user's country. The metadata provided by Google to the third-party app store would *not contain any user data***.** Requiring Google to share user data with third-party app stores would raise very significant security, privacy, and regulatory concerns. Google does not understand the proposed injunction to suggest that Google would be required to share user data as part of the catalog access remedy. Nor would the metadata provided by Google include any data generated by Google itself, like auto-translations, age ratings, or install counts. *Id.*

Google would provide the catalog data to the third-party app stores using the method described above rather than through a method that directly connects Play's catalog into the third-party app store, because that approach would require far deeper technical integration with Google's competitors than the method described above. *See* Baccetti Decl. ¶¶ 28-30. A direct connection to Play's catalog would require establishing and maintaining server-to-server or client-to-client connections between Google and the third-party app stores, effectively partnering the technical operations of Google with those of its competitors. This level of integration goes far beyond what is necessary to provide access to the Play store catalog. And this approach would increase the complexity, implementation time, and cost for Google and likely also for third-party app stores because it would require integration of the third-party app store's discovery function with Google's systems. This approach would also require Google to build, support, and maintain

servers to handle the traffic of users browsing another app store. Finally, this method of implementation would deprive third-party app stores of the ability to differentiate themselves from competitors by organizing and building their own discovery functions, recommendations, and merchandising capabilities within their storefront. *Id.*

Building and implementing Google's proposal for catalog access as described above would be extremely challenging and costly. *See* Baccetti Decl. ¶¶ 32-35; Cramer Decl. ¶ 12. Google could have to build and implement a system to aggregate and export metadata for approximately 3 million apps, as well as a system to refresh that metadata. Google would also be responsible for communicating with the approximately one million developers who list their apps in the Play store about the details of the catalog access program and the options available to them. Google would also have to tailor the metadata provided to the third-party app stores enrolled in catalog access based on the responses of each developer. Depending on the number of third-party app stores that enroll in catalog access, this could be incredibly burdensome—there are hundreds of third-party app stores on Android today. Cunningham Decl. ¶ 71. Google would have to repeat this process as developers list new apps in the Play store and as new third-party app stores elect to participate in the catalog access program.

Google would also have to devote resources to developing a billing system, onboarding third-party app stores, and creating a policy enforcement team to ensure compliance by third-party app stores with terms of service and developer preferences. Based on the information currently available to Google, and in the limited time available, Google estimates the total cost of building and implementing this remedy to be approximately $13.6 million to $23.7 million. Cramer Decl. ¶ 12. In addition, Google estimates an ongoing maintenance and policy enforcement cost of $7.5 million to $27 million, depending on the duration of the injunction. *Id.* It is Google's practice in its quarterly planning exercises to build in a 20-30 percent buffer to account for unforeseen costs. Applying the same approach here brings the total cost of this remedy to $27.5 million to $65.9 million. *Id.* It would take Google 12-16 months to implement this remedy. Baccetti Decl. ¶ 36.

B. Developer Consent Mechanism

The second aspect of Google's technical implementation of this remedy would be to build a mechanism to obtain developer consent to participate in catalog access generally, and specifically for particular third-party stores. This could be accomplished through a checkbox that developers can select to include an app in the catalog access program generally, as well as individual checkboxes allowing developers to identify the authorized third-party app stores that would have access to the app metadata through the program. Google would send a message to all developers upon implementation, as well as periodic updates as additional third-party app stores enroll in the catalog access program. *Id.* ¶¶ 19-20.

At the May 23 hot tub proceeding, Epic's expert proposed an "opt out" rather than opt in approach for this developer consent. In this context, "opt out" is both practically unwarranted and legally insufficient.

From a practical perspective, catalog access would fundamentally change Google's relationships with app developers. Since the launch of Android Market, the Play store's relationships with developers have been premised on Google's distribution of the developers' apps only in the Play store. This limitation is set forth in the Developer Distribution Agreement ("DDA"), Baccetti Decl., Ex. A, and in the commercial agreements that Google enters with app developers regarding the distribution and the use of their intellectual property. In addition, some developers enter into sublicenses of the intellectual property of third parties (e.g., the property of a movie studio or music producer) for purposes of distributing their apps, and those sublicenses may themselves limit the developer's distribution authority when it comes to app stores. *See* Baccetti Decl. ¶¶ 20-21.

The catalog access remedy would upend this premise for all developers, with enormous implications. Developers would now have to assess the scope of their own intellectual property sublicenses, the reputational and regulatory concerns associated with distribution of their apps in other app stores, and (potentially) the capabilities and nature of every third-party app store that participates in catalog access. If the Court adopts Epic's request for a worldwide injunction, developers would suddenly face a host of regulatory and compliance risks associated with

advertisement and distribution of their apps around the world. And Google would have to explain all this to the developers—what the program is, how it works, the options available to developers, and so on, in many different languages. Under these circumstances, it is not reasonable to assume that developers consent to have their apps distributed in every third-party app store that participates in catalog access unless the developer affirmatively opts out.

Moreover, Google would have no way to enforce a developer's decision to de-list their app from a particular third-party app store. Baccetti Decl. ¶¶ 21-22. Once the initial tranche of metadata associated with the Play catalog has been sent to a third-party app store, Google would have no way to claw that metadata back, and so even if a developer's app is removed from the next tranche, the third-party app store will still have all the metadata from the previous updates. While Google would make it a condition of terms of service for catalog access that third-party app stores abide by developer decisions, Google would have no technical way to prevent the third-party app store from continuing to use the metadata already in its possession. As a result, in certain circumstances, the third-party app store may be able to use that metadata to continue listing the developer's app in the store, notwithstanding the developer's decision to opt out.

As a legal matter, implementing catalog sharing on an opt-out basis would violate developers' intellectual property rights. Developers own substantial IP rights in their apps, including copyrights on the software and trademarks for brand features like logos and other images. The DDA grants Google a nonexclusive license to use developers' IP "in connection with" "the operation and marketing of Google Play." DDA § 5.1 (copyrighted software products); *see also id.* § 6.2 (comparable license for brand features, including trademarks). Google has no ability under the DDA to sublicense developers' content to third-party app stores. On the contrary, Google's only sublicensing authority is a highly limited sublicense permitting Google to allow third-parties to perform certain security functions, *see* DDA § 5.1(e), and developers expressly state that Google possesses no other "right, title, or interest" from developers. DDA §§ 4.4, 6.1.

Implementing catalog sharing would thus exceed the scope of Google's rights to developers' IP under the DDA, as Google would now be using the intellectual property of

developers in connection with the operation of third-party app stores, by providing the third-party app stores with the metadata necessary to list those apps in their stores. This Court lacks authority to compel non-party developers to grant third-party app stores the necessary licenses, or to compel them to grant Google the ability to sublicense their content to third-party stores. The Court's injunctive power extends only to Google and any non-parties working "in active concert or participation" with Google. *See* Fed. R. Civ. P. 65(d). This is a demanding standard, and Epic has not attempted to show that the test is satisfied with respect to non-party developers. *See Comedy Club, Inc. v. Improv West Assocs.*, 553 F.3d 1277, 1287 (9th Cir. 2009) (narrowing injunction improperly imposed on non-parties). Thus, to the extent the Court is inclined to order catalog sharing, it must do so on an opt-in basis, which would ensure that developers have consented and granted third-party stores the necessary licenses to distribute apps.

C. Fee for Catalog Access

The third aspect of Google's technical implementation of the catalog access remedy would be to develop and implement a model for charging third-party app stores for the services provided by Google through catalog access. Epic's proposed injunction does not state (as it does in the provision regarding distribution of third-party app stores) that Google may not charge such a fee.

As discussed above, Google estimates that it would cost approximately $27.5 million to $65.9 million to build and implement catalog access and to provide ongoing maintenance support and policy enforcement for the duration of the injunction. Those costs do not include the billions of dollars in costs that Google has incurred to build the enormous catalog that its competitors would now be permitted to access, nor does it account for the likely strategy of third-party app stores only developing direct relationships with apps that execute in-app transactions for digital services, meaning Google Play will supply all free apps without the potential of earning any revenue in return. These costs weigh strongly against an order compelling Google to implement this remedy at all. But if Google is forced to implement catalog access, then it must be permitted to charge third-party app stores for the significant services and value that Google is providing. An injunction to the contrary would amount to an order that Google perform valuable work for its competitors for free.

D. Eligibility Criteria

Finally, as part of its implementation of catalog access, Google would need to develop eligibility criteria for third-party app stores to mitigate the risk that catalog access would legitimize app stores that distribute malware, violate the intellectual property of developers through pirated or "unlocked" versions of apps (for example, an unauthorized version of a subscription app with the subscription requirement removed so that the user can access the content in the app for free), or otherwise promote illegal activity or objectionable content (e.g., pornography, hate speech). Google would also need to develop and implement an ongoing audit and enforcement system to ensure that third-party app stores enrolled in catalog access continue to meet those criteria. *See* Baccetti Decl. ¶¶ 23-24.

There are hundreds of third-party app stores that vary in terms of quality, sophistication and policies with respect to objectionable or illegal content. *See* Cunningham Decl. ¶¶ 71-75. App stores that traffic in malware or pirated content often have fewer apps in their catalogs because app developers do not want to legitimize these stores or associate their apps and brands with them. Without eligibility criteria, this proposed remedy would require Google to provide such app stores with the ability to appear like legitimate app stores, and would effectively place Google's imprimatur on them by showing the user a full catalog of apps from Play in those stores and funneling users to Play-branded pages.

As the technical implementation discussion above makes clear, such ill-intentioned app stores could then intermingle the apps from Google's catalog with malware or pirated apps from their own catalog, so that users are unable to distinguish legitimate Google-provided content from these app stores' objectionable or illegal content. This would harm Android users, who would be more likely to download malware that is intermingled with Google's catalog. It would also harm app developers both financially and reputationally, as pirated versions of their apps would be downloaded at higher rates when those pirated versions sit next to legitimate Play catalog apps. It would harm Google and the Play store, whose brands would be tarnished by having the Play store catalog mixed with unlawful or objectionable content. And it would harm Android, by increasing the prevalence of malware and pirated content in the ecosystem.

This is not a theoretical problem. Android app stores that traffic in malware or pirated content exist today. For example, HappyMod is an app store dedicated to hosting "modified" apks—that is, pirated, unlocked, or cracked—Android apps. Cunningham Decl. ¶ 72. Allowing these apps to flow through Android app stores using Play's trusted brand and catalog would further harm competition between Android and Apple's iOS.

To partially mitigate these harms, Google would create and implement a set of eligibility criteria for third-party app stores requesting catalog access, and a system to implement and enforce the criteria. *See* Baccetti Decl. ¶¶ 23. At a minimum, those criteria would include that an app store has: (1) a minimum number of apps in its own catalog and the basic infrastructure in place to conduct app store business; (2) bans on malware, pirated apps, and other illegal content; (3) procedures in place to enforce those bans; and (4) reasonably sufficient safeguards to protect the exported metadata.

The eligibility criteria would also include an agreement to terms of service with Google. Terms of service would be necessary to ensure compliance with local laws and regulations, and to address the novel questions arising from the unprecedented forced partnership between Google and its competitors created by catalog access. As noted above, terms of service are critical to mitigate the risk that third-party app stores will not abide by developer requests to remove their apps from catalog access. Such terms of service would also address other possible topics of dispute between Google and third-party app stores around catalog access, such as: unauthorized redistribution of the catalog metadata; responsibility for addressing developer complaints; responsibility for customer service; use of Google's brands and trademarks; and destruction of the catalog metadata when the injunction expires. Google must be able to require qualifying third-party app stores to abide by terms of service that address these and scores of other questions that are likely to arise during and after the period of any imposed injunction. And Google must be able to enforce those terms of service, including by disqualifying violating third-party app stores.

III. LIBRARY PORTING

Epic's proposed injunction requires "Google to provide users with the ability, subject to a one-time user permission, to change the ownership" for any or all apps installed by the Google Play store "such that the Third-Party App Store becomes the update owner for those apps." Proposed Injunction § II.D.1.

The existing capabilities of Android largely address the goal of the library porting remedy. Android 14 already enables third-party app stores to request user permission to update apps installed by other app stores. The additional permissions required by Epic's proposed injunction—to allow for bulk transfer of updating permissions and to allow app stores to change the ownership of all apps, including apps that are not distributed by the third-party app store—are unnecessary and would have serious negative consequences for the security of Android users and would impose significant costs and technical work on Google.

A. Existing Capabilities of Android 14

Epic's proposed remedy is unnecessary because Android's controls over cross-store updates already allow most of what Epic refers to in its proposed injunction as "library porting." Prior to Android 14 (released in October 2023), any preloaded app store on the user's device could update any app on the device without user permission or notification. For example, if the user had three preloaded app stores on the device, all three app stores could attempt to automatically update any app that was installed by the user from any app store. When app stores push updates to apps that the user expects to be updated via a different app store, problems for the user can arise. Such unauthorized cross-store updates, sometimes called "app clobbering," can result in loss of the user's prior in-app purchases or purchased subscriptions, and could cause apps to crash more frequently. Unauthorized cross-store updates can also create problems for developers, for example by frustrating their efforts to roll out new versions of their apps to a fraction of their user base in the first instance in order to ensure that any bugs in the new version are fixed before the new version is released more broadly (a process known as staged release). Cunningham Decl. ¶¶ 5-10.

To address these problems, Android 14 introduced the concept of "update ownership." This concept allows an app store to protect the user by requiring user confirmation before a

different app store can update apps installed from that app store. In other words, any app store can ensure that, by default, an app installed from that app store will receive automatic updates only from that app store unless and until the user decides otherwise. But any app store on the device can request user permission on an app-by-app basis to update an app that was installed by another app store when the new store has a compatible update available. When "update ownership" is cleared from the app, any app store on the device (including but not limited to the app store that requested the permission) can then update the app. *Id.* ¶¶ 11-14.

These existing features of Android largely achieve the goal of library porting as described by Epic's expert. In his statement, Dr. Bernheim explains that the purpose of library porting is to "allow[] users to transfer the responsibility of updating apps that were originally downloaded from the Google Play Store to the third-party app store such that the third-party app store would be responsible for automatic updates of apps (and would from that point forward be entitled to any ongoing revenues from the developer)," resulting in "competition between Google Play and its rivals" that "will directly benefit users." ECF No. 952-1, Bernheim ¶ 64. Android allows third-party app stores to update apps in this way by requesting permission from the user to "clear ownership" on an app-by-app basis. Cunningham Decl. ¶¶ 11-14. This app-by-app permission requirement is not particularly burdensome on the app store because there is no limit to the number of update requests that an app store can send the user. And if the developer has provided the third-party app store with a version of the app that incorporates the third-party store's billing system (or has otherwise complied with that app store's policies on billing), then the third-party app store could start collecting service fees on in-app purchases (assuming it collects a fee for equivalent digital goods and services) once it has updated the app on the user's phone with that version.[3]

[3] As discussed in Mr. Cunningham's declaration, developers must take certain actions with respect to their apps to allow for the possibility of third party app stores updating their apps, thereby receiving "ongoing revenues" as Dr. Bernheim describes. In particular, the developer would have to provide the third party app store with updated versions of the developer's apps incorporating the third party app store's billing system. The developer would also have to ensure that the Android operating system recognizes the third party app store's version of the app as the same app that the user acquired from a different app store. As Mr. Cunningham's declaration explains, the

B. Changes Required to Implement Remedy

Epic's library porting proposal would require the addition of two capabilities that do not currently exist in Android 14. The first is a bulk update request (described by Epic as a "one-time User permission" to change ownership for all apps on the phone).[4] The second is a "change ownership" permission rather than a "clear ownership" permission. These changes would significantly harm Android users and impose substantial technical work and costs on Google.

1. Bulk Update Request

The Android operating system requires app stores to request permission to clear ownership on an app-by-app basis when the third-party app store has a compatible update available, rather than (as Epic has proposed) through a bulk request. To implement the "one time User permission" requirement of Epic's proposal, which would require *bulk* ownership change of apps on the user's device, Google would have to modify the Android operating system. Specifically, Google could introduce a new Android API to request a bulk ownership change, with a corresponding "behind-the-scenes" permission that app stores would declare in their app manifest and that governs the use of this API. When this API is invoked along with a list of app package names, the API would display a user interface that the app store could use to seek user consent to perform updates to one or more apps without the per-app update ownership dialog prompt. The actual change in update ownership for each app would be deferred until the app store successfully installs an update for each app. Cunningham Decl. ¶ 19.

This change to Android 14 would harm users. The app-by-app approach to cross-store updates was designed to give users a straightforward decision they can make quickly and easily one app at a time. This approach makes sense because users may have good reasons to prefer to have different apps updated by different app stores. For example, App Store A may offer

---

developer could accomplish this in several ways, including through the use of a single signing key for the app across app stores. Cunningham Decl. ¶¶ 33-39.

[4] Google understands the term "one-time User permission" to mean that an app store can issue a single update ownership request for a group of apps already installed on the phone, and not that an app store can issue a single request for permission to automatically update all apps acquired from any source in the future. The latter interpretation would lead to a host of additional problems discussed in Mr. Cunningham's declaration. Cunningham Decl. ¶ 22.

exclusive content for one app on a user's device, while App Store B may offer promotional discounts for a different app on a user's device. This is consistent with the way users already make decisions about installation of apps on their device–one app at a time. By contrast, requiring the user to make a single decision about all the apps on their device at one time is likely to confuse the user. Indeed, a user presented with a "one-time User permission" to update all apps on the device from a single app store may not realize that the consequences of agreeing to that request will be to lose protection against having *any* app store update *any* app on the device. *Id.* ¶ 18.

To mitigate these harms, if Google were ordered to implement this change to the Android operating system, Google would also modify the operating system to permit the developer to choose whether to allow its apps to be subject to the new bulk ownership change protocol. Google would do this by giving developers the ability to indicate in the code of their APKs whether the app can be transferred in bulk along with other apps, or if instead the per-app permission would continue to apply to that app. Google would also give the developer the opportunity to indicate in the code of the APK which third-party app stores are permitted to obtain ownership over the app by means of the bulk transfer. *Id.* ¶ 20.

2. Change Ownership

The second change to the Android operating system that would be required by Epic's proposed injunction is to add a "change ownership" capability. As described above, the Android operating system does not allow a user to "change the ownership" of an app from one store to another. Instead, Android enables a user only to "clear ownership" of an app so that the app can be updated by *any* app store, not just the app store that requested the update permission, without any further authorization by the user.

If Google were ordered to implement Epic's "change ownership" proposal, Google would create a capability in the Android operating system to perform the update owner switch. Google would also create a new "update ownership" dialog, design, and language to accommodate this change in behavior. *Id.* ¶ 30.

Here again, Epic's proposed change would harm Android users. *See id.* ¶¶ 24-27. The proposed "change ownership" permission (unlike "clear ownership") would allow only the app

store that requested the permission to update the app. The problem is that an app store could ask a user to "change ownership" of an app that the app store does not actually distribute. (The Android operating system has no way to tell whether an app store actually distributes any particular app, and so the operating system has no way to limit the "change ownership" permission to an app store that actually distributes the app.) In that circumstance, the user would stop receiving updates for the app. This would lead to several harms. First, the app developer (who has no association with the third-party store) would be unable to push updates out to its users, significantly harming the developer's business. Second, users would stop receiving security updates. Many apps, including banking apps, push updates to users on a regular basis to patch security holes. Mr. Cunningham describes a recent example in his declaration. *Id.* ¶ 26.

If users were unable to obtain these kinds of security updates—because an app store that does not actually distribute the app has convinced the user to "change ownership" of the app—the results could be disastrous for the user. These risks would not be apparent to a user who is simply shown a dialog box asking for permission to "change ownership." Android 14 addresses these risks by allowing an app store to request user permission to "clear ownership" on an app-by-app basis, but not "change ownership" for a user's entire set of apps. As discussed above, the "clear ownership" permission does not prevent another app store from updating the app, thereby preventing the scenario described above. *Id.* ¶ 27.

The risks to users associated with Epic's proposed "change ownership" permission are even greater when considered alongside Epic's proposed "bulk update" permission. If Google were required to implement both of these changes to Android 14, then an app store could send a one-time user permission to "change ownership" of every app on a user's device, including apps that the third-party app store cannot update. At that point, every app on a user's phone will be incapable of updating, potentially including apps that are integral to the functioning of the phone. *Id.* ¶ 28.

Here again, if Google were ordered to modify the Android operating system to implement Epic's "change ownership" proposal, then Google would also have to build some protections into the operating system to mitigate these harms. Google would do so through a developer choice

protocol similar to the "one time User permission" mitigation discussed above. A developer could embed a statement inside the APK file indicating whether ownership of the APK can be transferred, and if so which particular app stores are authorized to change ownership of the app. OEMs and carriers could configure the same permission for apps they preload. *Id.* ¶ 30. This approach is consistent with the provision in Epic's proposed injunction that the new store would become the "update owner" of bulk-transferred apps only "if and when those apps become available on the Third Party Store." These protections would potentially mitigate, but not eliminate, the harms to the user that may arise from an app store taking advantage of the single permission to take control of apps.

C. Costs of Library Porting

These changes to the Android operating system would be very costly. Changes to the Android operating system are enormously consequential. The operating system is the underlying software that powers billions of Android phones. An error or bug in the operating system can have disastrous consequences for users, developers, OEMs and Google. Accordingly, changes to the Android operating system that involve behavior changes to APIs and that impact external developers, like those that would be required to implement Epic's proposed remedy, require extensive developer previews, beta testing, feedback from users and OEMs, and final bug fixes prior to a public release.[5] Because these tasks must be scheduled well in advance and take several months to complete, Google sets a regular cycle for Android updates. *Id.* ¶ 47.

Making the changes to the Android operating system proposed by Epic earlier than that would not be feasible. New features implemented into the operating system take time to build in a way that avoids unintentional regressions in device functionality, including unforeseen interference with the operation of users' apps. It takes time to test out the changes and establish the possible app compatibility impact, and it takes time for impacted app developers to make necessary adjustments to their apps as well. Google's testing of changes to the Android operating

[5] More minor changes to the Android operating system–like enhancing screen sharing functionality or adding an option from the "quick settings" panel to share Wi-Fi credentials–occur on a more frequent cadence.

system includes public developer preview and beta programs to ensure that the changes operate as intended. Google solicits feedback from developers and users participating in these programs to identify bugs and other issues. These programs take several months, and there is no way to fast track them because this kind of testing requires users to operate their devices in the ordinary course over a period of time. *Id.* ¶ 49-51.

Another important aspect of the operating system testing process involves OEMs, since it is the OEMs that ultimately decide whether to adopt Android changes in their updates or new releases. OEMs engage in significant engineering work to assess and integrate changes, typically also implementing their own testing programs. In many countries, there is yet another level of testing conducted by mobile carriers. The timing of OEM and carrier testing of new versions of the operating system is not within Google's control. *Id.* ¶ 49-52.

The technical costs to implement and maintain these changes to Android would be approximately $1.7 million to $2.4 million. Cramer Decl. ¶ 13. If Google were ordered to implement these changes off-cycle, the cost to Google would be far higher, as Google would have to initiate a separate round of user, developer, and OEM testing and feedback described above. Cunningham Decl. ¶ 53.

IV. DISTRIBUTION OF THIRD-PARTY APP STORES

Epic's proposed injunction would require Google, for a specified period of time, to "allow distribution of competing Third-Party App Stores on the Google Play Store." ECF No. 952, Proposed Injunction § II.D.2. Under the proposed injunction, Google would not be permitted to charge third-party app stores for this service. *Id.* § II.D.2.ii. The details of technical implementation of distribution of third-party app stores discussed below show several of the problems associated with this proposed remedy.

Google's implementation of this proposed remedy would involve four steps: (1) redesign the Play store to accommodate the distribution of app stores; (2) implement a thorough ongoing vetting process for the policies, conduct and catalogs of app stores that request to be distributed through the Play store; (3) change the Android operating system; and (4) build and implement a charging model for third-party app store distribution.

A. Redesign of the Play Store

The Play store as it exists today is designed to distribute apps, not app stores. This change would require a fundamental redesign of the Play store. As explained in the declaration of Mr. Baccetti, that redesign would include the following steps. Google would have to reconfigure the Google Play Console to allow developers to declare an app as an app store, agree to abide by Play store policies, and accept additional terms of service. Google would also have to create ways for the Play store to handle the display of app stores within the store and design a method to track and identify for users which apps in the store are "app stores." And Google would have to build and implement a warning that advises users when they are about to download an app store. *See* Baccetti Decl. ¶¶ 38-41.

B. Vetting Process

Google would implement a thorough vetting process for app stores requesting distribution through the Play store. This vetting process would likely include three components: (a) initial and ongoing review of all apps and updates in the app store's catalog for compliance with Play's security and content policies; (b) initial and ongoing review that the app store meets criteria set by Google to qualify as an "app store"; and (c) initial and ongoing review that the app store complies with behavior policies set by Google.

1. Review of App Store Catalogs

As Dave Kleidermacher testified at trial, and as summarized in his declaration, the Play store performs a human review of all new apps to determine compliance with Play's security and content moderation policies. Kleidermarcher Decl. ¶ 8. The Play store also employs a sophisticated infrastructure that conducts a machine-based review, scrutinizing the application and the developer for signals of risk that would trigger further human review. Google also reviews all app updates using a machine-based review. An app or update is not published until the Play store completes these reviews. Millions of apps and updates are submitted to the Play store annually, and Google conducts the review described above for all those submissions. This app review process is an integral component of the Play store business model and the Google brand. *Id.*

If Google were ordered to distribute third-party app stores through the Play store, then Google would subject the catalogs of those third-party app stores to the same rigorous review, because the content of those stores would now be accessible through the Play store. This would include a thorough review of the third-party app store's catalog at the time the store first requests distribution through Play. Once the third-party app store is listed on Play, Google would conduct the same review for every update to every version of every app in the third-party app store, as well as every app that the third-party app store proposes to add to its catalog, before the app can appear in the third-party store. No app or update could be published in a third-party store distributed through the Play store until Google has cleared that app or update for compliance with Google's safety and content policies. *Id.* ¶ 9. Google would be required to devote substantial resources to enforcing the outcomes of this rigorous review, both by instructing third-party app stores to remove non-compliant apps and updates and by potentially removing app stores that did not comply with Google's review process from Play.

The risk to the Play store and Google brands posed by the distribution of third-party app stores is not a purely theoretical concern. As noted above, there are hundreds of Android app stores today, some of which list and even promote content that violates the Play store's policies. Mr. Cunningham notes in his declaration, for example, the Nutaku Android store advertises itself as "the world's largest 18+ gaming platform," and features apps with adult content. Cunningham Decl. ¶ 74. Similarly, Aptoide (another Android app store) hosts adult apps including Pornhub and an unrestricted version of Telegram that allows adult content, as well as pirated apps. *Id.* HappyMod is an example of an Android app store dedicated to distributing pirated or "unlocked" versions of Android apps and games. *Id.* ¶ 72. And CepKutusu.com was an example of an app store that intentionally distributed malware, incorporating banking malware into every app downloaded from the store. *Id.* ¶ 73. If users were able to access this type of content through the Play store by downloading these app stores from Play, the reputation for safety, security, and content moderation that the Play store has spent over a decade and billions of dollars building would be irreparably damaged.

At the May 23 hot tub proceeding, the Court suggested that Google could show a screen to a user who is about to download a third-party app store from the Play store disclaiming any responsibility for the consequences. While Google certainly would want the ability to implement such a warning, that alone is far from sufficient to protect users, for the same reason that it is not enough simply to show such a screen when a Play user downloads an app. Kleidermacher Decl. ¶ 23. The brand and reputation of the Play store are built on providing users with a safe, secure, reliable experience, not on disclaimers. That experience includes browsing the Play store, downloading the app, and safely using the app after it is downloaded. A "buyer beware" disclaimer does not repair the harm to the Play store's brand when a child is able to view adult content through an app store acquired from Play, or when a user's device is infected with malware from an app store acquired from Play as a result of this proposed remedy. In those scenarios, the Play store is the platform that connects the user with the app stores that inflict those harms. It is unrealistic to expect that the user will not blame the Play store at least partially for those harms, just as it is unrealistic to expect that a user will not blame the Play store at least partially for harms inflicted by an app downloaded directly from the Play store. If users are exposed to unsafe content through Play on Android, users will naturally consider other options they perceive to be more secure, such as Apple's iOS.

2. App Store Criteria

Google's vetting process would also include a definition of what constitutes an "app store" for these purposes. In connection with this protection, Google would set criteria as to which apps are eligible to be distributed as app stores through the Play store. Such criteria are necessary to mitigate the risk that any number of apps on Play would immediately build in the capability to start installing other apps on the devices of users with a single one-tap screen. The evidence at trial showed that Epic distributes its game Fortnite on Android using the Epic Games Launcher, a separate app that has the capability to install Fortnite on a device. This proposed remedy would allow a developer like Epic to avoid Google's service fee simply by distributing the launcher on the Play store as a "third-party app store." To avoid this scenario, if this remedy is implemented over Google's objection, then Google must be allowed to set eligibility criteria for

app stores distributed through the Play store, including prohibiting "launchers" like the Epic Games Launcher, so that developers cannot evade any obligation to pay for the value of the Play store simply by calling their app an app store. *See* Baccetti Decl. ¶¶ 40-41.

3. Behavior of App Stores

Google's vetting of third-party app stores would also include compliance with terms of service setting guidelines for the behavior of app stores distributed through the Play store. For example, one of Google's criteria for app store distribution would be that the third-party store does not automatically install apps on a device that the user has not expressed an intention to install. One recent example of this was the Redstone installer, a pre-installed system app on Android mobile devices sold in Germany that automatically installed malware on the device. Kleidermacher Decl. ¶ 13.

C. Change to Android Operating System

This remedy as described in Epic's proposed injunction would also require a change to the configuration of installer permissions in the Android operating system. Currently, Android has two installer permissions: INSTALL_PACKAGES and REQUEST_INSTALL_PACKAGES. INSTALL_PACKAGES is granted by the OEM when it configures the device. For example, on a Samsung Galaxy Phone, the Samsung Galaxy Store and the Play store are preinstalled with INSTALL_PACKAGES when the device is shipped. INSTALL_PACKAGES allows the app store to install other apps on the device without requesting user permission for each install. Cunningham Decl. ¶ 57.

REQUEST_INSTALL_PACKAGES does not require OEM permission–any app can configure itself to request this permission from the user. For security reasons, each time a user attempts to install an app through another app that has the REQUEST_INSTALL_PACKAGES permission, the user is shown a consent screen. The purpose of this distinction between the two installer permissions is to protect the user from a malicious app installing other apps (including malware) in the background without the user's knowledge or consent. App stores downloaded from the Play store would have the REQUEST_INSTALL_PACKAGES permission (because they were not configured on the device by the OEM), and therefore each time a user installs an app

through an app store acquired from the Play store, the user would see a consent screen. *Id.* ¶ 58. This would appear to violate Section II.D.2.i of the proposed injunction, although the language of this provision is not entirely clear.

To implement this change, Google would remove the need for user confirmation for installation of apps, and add a new behind-the-scenes permission that app stores would add to their manifest. To partially mitigate security vulnerabilities arising from this change, Google would likely add a technical restriction that the new permission must be granted by the installer of the app store itself. For app stores distributed through the Play store, this would mean that Play would grant the third-party app store the permission exempting that app store from the per-app confirmation dialog.[6] *Id.* ¶¶ 61-63.

D. Charging Model

Finally, if Google were forced to implement this remedy, Google would build a model for charging third-party app stores for distribution on Play.

The provision in Epic's proposed injunction stating that Google cannot charge for app store distribution is entirely unwarranted. This proposed remedy would require Google to provide valuable services to competitors on an ongoing basis for free. The evidence at trial showed that the Play store's business model is to provide benefits to app developers and to receive compensation for those benefits through a service fee on in-app purchases within apps downloaded from the Play store. The evidence showed that this is a very common business model among app stores on various platforms, including the Epic Games Store on PCs. An injunction stating that Google cannot charge third-party app stores for distribution through Play would mean that Google would be required to provide these valuable services to its competitors—using Google's proprietary systems and intellectual property—for no compensation whatsoever. This outcome is particularly drastic when considered in tandem with the other proposed remedies discussed in this proffer, which would force Google to provide valuable services to competitor app

[6] In addition, to lessen the risk of silent background installation of harmful and unwanted apps, Google may also require that installing a new app (without a confirmation dialog) be permitted only in response to a proactive install decision by the user, for example by tapping an "install" button that the store renders for the user. Cunningham Decl. ¶ 64.

stores while giving those app stores a mechanism to deprive Google of the service fees that reflect its compensation for those services. Considered together, these remedies amount to an unprecedented forced subsidy to Google's competitors.

E. Total Cost

As explained in Mr. Cramer's declaration, Google estimates that the cost to reconfigure the Play store to distribute other app stores would be $15.1 million to $18.5 million. In addition, the cost of ongoing maintenance, policy, and policy enforcement support would be $9.1 million to $32.2 million, depending on the duration of the injunction. Building in a buffer of 30 percent of the cost, which is Google's standard practice in quarterly planning exercises, yields an aggregate total cost of $31.4 million to $66.7 million. *See* Cramer Decl. ¶ 14. The additional changes to Android to accommodate this remedy would also be between $628 thousand and $751 thousand to build and implement, and then between $79 thousand and $282 thousand to supervise and maintain depending on the injunction's duration.

On top of that, the cost to vet other app stores for distribution on Play would depend on the number of apps in the app stores that were not already in the Play store. Without knowing details about the catalogs of the app stores that would apply for distribution through the Play store, it is impossible to estimate the cost of this vetting. The most Google can say is that the cost of that vetting would depend on the degree to which the vetting of the catalogs of third-party app stores increases Google's current app review process. Mr. Kleidermacher estimates that Play's app and update review process, at its current level, costs approximately [redacted] annually. Kleidermacher Decl. ¶ 14. If the vetting associated with distribution of third-party app stores resulted in a 20 percent increase in Play's app and update review workload (and Mr. Kleidermacher believes that is a reasonably likely possibility), then the cost to Google would be [redacted] annually. For an injunction lasting two to six years, that would cost Google between [redacted] and [redacted].

DATED: June 24, 2024

Respectfully submitted,

By: */s/ Glenn D. Pomerantz*
Glenn D. Pomerantz

MUNGER TOLLES & OLSON LLP
Glenn D. Pomerantz
Kuruvilla Olasa
Jonathan I. Kravis
Justin P. Raphael
Nick R. Sidney
Dane Shikman
Rebecca L. Sciarrino
Jamie B. Luguri
Lauren N. Beck

MORGAN, LEWIS & BOCKIUS LLP
Brian C. Rocca
Sujal J. Shah
Michelle Park Chiu
Minna Lo Naranjo
Rishi P. Satia

HOGAN LOVELLS US LLP
Neal Kumar Katyal
Jessica L. Ellsworth

Counsel for Defendants

E-FILING ATTESTATION

I, Glenn D. Pomerantz, am the ECF User whose ID and password are being used to file this document. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that counsel for Defendants have concurred in this filing.

s/ Glenn D. Pomerantz
Glenn D. Pomerantz

EXHIBIT K

Brian C. Rocca, S.B. #221576
brian.rocca@morganlewis.com
Sujal J. Shah, S.B. #215230
sujal.shah@morganlewis.com
Michelle Park Chiu, S.B. #248421
michelle.chiu@morganlewis.com
Minna Lo Naranjo, S.B. #259005
minna.naranjo@morganlewis.com
Rishi P. Satia, S.B. #301958
rishi.satia@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105-1596
Telephone: (415) 442-1000

Neal Kumar Katyal, *pro hac vice*
neal.katyal@hoganlovells.com
Jessica L. Ellsworth, *pro hac vice*
jessica.ellsworth@hoganlovells.com
HOGAN LOVELLS US LLP
555 13th St. NW
Washington, D.C. 20001
Telephone: (202) 637-5600

Counsel for Defendants

Glenn D. Pomerantz, S.B. #112503
glenn.pomerantz@mto.com
Kuruvilla Olasa, S.B. #281509
kuruvilla.olasa@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, CA 90071
Telephone: (213) 683-9100

Justin P. Raphael, S.B. #292380
justin.raphael@mto.com
Dane P. Shikman, S.B. #313656
dane.shikman@mto.com
Rebecca L. Sciarrino, S.B. #336729
rebecca.sciarrino@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty Seventh Floor
San Francisco, CA 94105
Telephone: (415) 512-4000

Jonathan I. Kravis, *pro hac vice*
jonathan.kravis@mto.com
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Ave. NW, Suite 500E
Washington, D.C. 20001
Telephone: (202) 220-1100

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION THIS DOCUMENT RELATES TO: *Epic Games Inc. v. Google LLC et al.,* Case No. 3:20-cv-05671-JD	Case No. 3:21-md-02981-JD **DECLARATION OF VITOR BACCETTI IN SUPPORT OF GOOGLE'S PROFFER REGARDING EPIC'S PROPOSED REMEDIES** Judge: Hon. James Donato

DECLARATION OF VITOR BACCETTI

1. I am a Group Product Manager at Google. In that role, I am responsible for app distribution at Google Play. The facts set forth herein are within my personal knowledge and if called as a witness, I could and would competently testify to them.

2. I am a Group Product Manager at Google. In that role, I am responsible for app distribution at Google Play. The facts set forth herein are within my personal knowledge and if called as a witness, I could and would competently testify to them.

3. I have reviewed the portions of Epic's proposed injunction relating to Catalog Access, Library Porting, and Distribution of Third Party Stores through the Play store. I offer this declaration to describe the technical implementation and anticipated resource allocation required for some of these remedies. This declaration reflects my current analysis within the short timeframe provided and based on the limited description of the remedies set forth in Epic's proposed injunction. If Google were ordered to implement these remedies, it is possible that Google could encounter unanticipated issues requiring different methods of implementation, which may entail a different resource burden and cost.

4. Because of my role, this declaration is focused on the changes that Google would need to make to the Play store in order to implement some of these remedies.

Catalog Access

5. In this section, I describe the technical means by which Google would implement the "catalog access" remedy if ordered to do so, as well as the resources required and timeline for implementation.

Implementation of Catalog Access

6. If Google were ordered to implement the catalog access remedy over its objection, Google could export metadata associated with the apps in its catalog, for which developers have opted in, to a server for authorized third-party stores to access. The authorized third-party stores could use that metadata to display those Play apps in their storefronts. If a user attempts to install a Play app on the third-party storefront, the Play store would facilitate and actually perform the installation. That app would be treated as a Play-installed app by Google going forward.

Metadata Export

7. There are over 1 million developers and around 3.2 million published apps on the Google Play store.

8. Google would regularly export metadata associated with these apps in its catalog to a server and refresh it on a daily basis. The metadata could include basic data pertaining to the app itself (e.g., app name and package name, developer name, image of app icon, and app category), as well as some basic information provided by the developer about the app, such as the countries in which the app is distributed and whether the app offers in-app purchases. The export would not include any user data, which includes reviews of the app given by other users. The export would also exclude data generated by Google, like auto-translations, age ratings, and install counts.

9. Subject to agreed-upon terms of service, including meeting reasonable eligibility criteria, Google could grant to authorized third-party app stores access and a limited license to this metadata for the purpose of displaying Play apps that are not already in the third-party app stores' own catalogs. Google could host this metadata to be accessible to an authorized third-party store's serving system.

10. Third-party app stores could populate their storefronts from both the metadata export of Play apps, and their own local databases containing apps published directly to their stores. When displaying apps to users, the third-party store could merge the results to create a single user-facing catalog inside the third-party's storefront.

Installation by Play Store

11. When inside the third-party storefront, if a user clicks to install an app that the developer distributes to that third-party store, then Play would have no involvement in fulfilling the install. When the user, by contrast, clicks to install a Play-sourced app that is displayed pursuant to the process described above, then Google would implement the following process to fulfill the installation.

12. If not already a Play user, users would be required to agree to relevant terms of service and be signed in with a Google account before proceeding to the app installation process. The same conditions apply for users when visiting the Play store through other means.

13. If the package does not exist, or the user or device is not one which the developer has permitted to install the app, then the user will see a message informing the user that the app is not available.

14. If the package exists and the user and device are ones which the developer has permitted to install the app, then a user interface will appear from Play that gives the user additional information about the app, and contains an install button if they are eligible to install the app. The user can install the app from that user interface, without leaving the third party store.

15. Google, rather than the third-party app store, would generate this user interface, with Play branding, so that the user is on notice that this app originates from the Play store and they are agreeing to Play's terms and conditions, just as if they were installing the app directly from the Play storefront itself. In addition, there are regulatory requirements in certain jurisdictions regarding the content of the information displayed to users at the point of install, and because Play is fulfilling the install then Google must ensure that it is meeting those requirements.

16. Google may also need to build and implement an additional security layer that ensures that the app store seeking to call the Application Programing Interface ("API") from Play that generates the overlay interface is, in fact, an app store that the developer has authorized to make the app available through catalog access. This mechanism would involve building and maintaining, in real time, a list of approved callers of the Play API described above. Google may also decline to serve requests for apps when the app's developer has not consented to share their metadata with the third-party store calling the API.

17. This process fulfills the requirement in Epic's proposed injunction that the install occur through a "background process similar to the Alley Oop integration offered by Google to certain third-party Developers." I was the product manager for some time for the "Alley Oop" project at Google, which is known externally as the Google Play App Access Program. This was a beta project that Google created for "publisher" developers—*e.g.*, Twitter, Pinterest, Facebook—

to integrate so that users who click on app install ads would not have to leave the publisher's app in order to have Play fulfill the install of the app being advertised. The install process I describe above to implement Epic's catalog access remedy would be very similar to our previous Alley Oop program.

18. Because the Play store is handling the installation and subsequent updates of the app, Google would treat the app exactly as if it was installed directly from the Play storefront. For example, the user can receive and redeem Play points for qualifying in-app purchases, and Play can communicate with the user to provide updates as well as notifications about Play store products and promotions, just like any other Play customer. Because the user installed the app from Play, the user would be considered a Play customer.

Developer Consent Mechanism on Developer Console

19. As part of its implementation of catalog access, Google would give developers a mechanism to provide consent to participate in catalog access through the Google Play Console. The Google Play Console is the platform that developers use to manage their apps in the Play store, including setting parameters for how and to whom the apps may be distributed. Google would also provide developers who opt in to catalog access with additional options that allow the developers to be more specific in selecting which authorized third-party app stores they want Google to give access to their apps.

20. Providing this consent mechanism for developers is critical. Developers may have reasons why they do not want their apps to be distributed by a certain app store, or in a storefront next to "unlocked" or pirated versions of the same apps, or in an environment with illegal or inappropriate content that may hurt the developer's brand, such as pornographic or violent content. Moreover, developers own IP rights in their apps, including the app icon image that Google would need to share with third-party stores. In addition, many developers *themselves* have licenses from other third-parties. For example, Kabam Games, Inc., relies on content from Disney and Marvel to distribute the "Marvel Contest of Champions" and "Disney Mirrorverse" games on the Play store. For these reasons, Developers need the right to control the distribution of their IP and the IP they have sublicensed. Based on my experience as a product manager for app distribution,

copying (or "scraping") the publicly available app information from the Play store, and then distributing unauthorized versions of those apps in other stores is common—and it is very frustrating for some developers.

21. If Google were to make developers' apps available to third-party stores *by default*, and merely allow an objecting developer to opt out of the program, this could present some practical problems for non-consenting developers. For example, it may be that a third-party store could have already obtained the developer's IP and metadata from an earlier Google export, *before* the developer noticed the option in the Play Developer Console or had time to opt out of the program. In that circumstance, there would be no way for Google to "claw back" that information—including potential trademarks in the developer's app icon—from a third-party store.

22. Not only could a third-party store make available a developer's app icon and associated information over the developer's objection, but it could assist users in installing the app through Play over Google's objection too. In particular, the third-party store could simply deep-link the user to the Play store install page, and the Play client would have no way of determining that the user originated from a store that the developer had not approved to receive the app through catalog access.

Eligibility Criteria and Terms of Use

23. As part of its implementation of catalog access, Google would likely seek to set eligibility criteria to ensure that only legitimate and safe app stores could obtain access to the approximately 3 million apps in Google's catalog. For example, Google works hard to protect data from leaks and hackers, so it may require that the third-party store have reasonably sufficient safeguards to protect developers' data that Google would be required, by this order, to export.

24. Moreover, without any eligibility criteria, any app could declare itself an "app store" and instantly get access to the millions of apps in Google's catalog, without actually resembling an app store in any sense. For these reasons, Google would implement eligibility criteria that would include, for example, a requirement that an app store has a minimum number of apps in its own catalog and the basic infrastructure to conduct app store business; a requirement

that the app store forbid malware, pirated or unlocked apps, and other illegal content; has catalog review procedures in place to enforce those rules; and has agreed to terms of use with Google.

Charging Model

25. If ordered to undertake the efforts described above, Google would build a fair and reasonable model for receiving compensation for this value, including the value of the catalog of Google's apps. I am aware of no precedent for a company providing its entire digital catalog for a competitor to display in its own storefront, as contemplated by Epic's proposed injunction, so it will take work to determine what a fair and reasonable fee model would be. This may include cross-functional efforts within Google to develop policies, assess relevant rules in various jurisdictions, evaluate third-party app store economics, and more.

26. Google will incur costs in connection with maintaining an infrastructure and processes to facilitate and manage commercial relationships with third-party stores. While some of those costs are fixed, others will depend in some measure on the number of third-party app stores that choose to participate in catalog access. That work will necessarily involve time dealing with these stores as a business customer, including dealing with disputes and, in some circumstances, potential escalations to senior executives. Depending on the fee model that Google adopted, Google may need to develop an infrastructure to identify and monitor eligible installs, as well as to invoice, audit, and securely process payments.

Alternative Approach

27. I believe the above-described model of implementing catalog access achieves the letter and spirit of what Epic's proposed injunction requests.

28. An alternative approach may be to directly connect Play's catalog and systems to the discovery functions of the third-party store. In essence, when a user is browsing or searching within a third-party storefront, the third-party store would query Play in real time in response to a user search prompt, and Play would deliver the necessary metadata that is specific to that request so that the third-party store can then process and render the information for the user. Google could achieve this either at the server level—connecting Google's servers with those of third-party stores—or at the on-device client level.

29. This approach has downsides for both Google and third-party stores. First, this would require Google to establish a deeper technical integration with its competitor app stores, partnering with those stores on the discovery function within their storefronts. This level of partnership increases the entanglement between Play and its competitors, and introduces additional opportunities for disputes, escalations, etc. Because of the added complexity and the need to collaborate more with third-party stores, it also may increase costs and time to implement the remedy.

30. Second, this approach would not involve giving access to Play's catalog, so the third-party store would not have that catalog to organize and build their own discovery functions within their storefront. Particularly, if a third-party store is seeking to differentiate from Play and compete for users, this approach would make that kind of differentiation more difficult because the third-party store would not have the ability to use the catalog to organize and build its own discovery functions, recommendations, and merchandising capabilities within its storefront.

31. Finally, this approach would require Google to build, support, and maintain servers to handle the traffic of users browsing another app store.

Estimate of Costs & Timeline

32. In this section, I address expected resource requirements, and timeline, to implement the catalog access remedy as described above. To make these resource requirement estimates, I am drawing on my experience as a Product Manager in the Google Play organization over the last 8 years, during which I have overseen the development of multiple features from inception to launch.

33. To implement this catalog access remedy, and then to maintain it on an ongoing basis for the duration required, I estimate the following resource commitments. These estimates assume that the export contains the types of app-related metadata described above, and that developers can consent on a per-app-store basis. Because we have never launched a program like catalog access before, I do not have a prior model on which to base these estimates, so there is some uncertainty about the specific resource requirements, but I have attempted to do our best to predict the resources that would be required to implement the remedy.

Resources / FTEs	Duration Required	Scope
Initial Scoping & Design		
1 Product Manager (PM)	3 months	Overall solution
1 Senior Software Engineer (SWE)	3 months	Overall solution
Implementation & Launch		
1 PM	6-9 months	Data sync & developer consent
6 SWE	6-9 months	Data sync & developer consent
2 SWE Eng Prod	6-9 months	Data sync & developer consent
1 Technical Program Manager (TPM)	6-9 months	Data sync & developer consent
1 Tech Writer (TW)	6-9 months	Data sync & developer consent
1 Legal Counsel	6-9 months	TOS / DDA / Other Policy
2 XFN Resources (Policy, Program Manager)	6-9 months	TOS / DDA / Other Policy
1 PM	6-9 months	TOS / DDA / Other Policy
1 SWE	6-9 months	TOS / DDA / Other Policy
1 PM	6-9 months	Installation User Interface and APIs
5 SWE	6-9 months	Installation User Interface and APIs
1 SWE Eng Prod	6-9 months	Installation User Interface and APIs
1 UX Designer	6-9 months	Installation User Interface and APIs
1 TPM	6-9 months	Installation User Interface and APIs
2 Business Dev Managers	6-9 months	Outreach and support for developer consent
Mechanism for More Frequent Updates		
7 SWE	6-9 months	Mechanism for lower latency refreshes of app metadata

2 SWE Eng Prod	6-9 months	Mechanism for lower latency refreshes of app metadata
1 TPM	6-9 months	Mechanism for lower latency refreshes of app metadata
Onboarding of Stores		
3 Technical Solutions Consultant/Engineer (TSC/TSE)	3 months	Partner support for integrating with metadata export and new APIs
1 TPM	3 months	Partner support for integrating with metadata export and new APIs
Build & Implement Charging Model[1]		
7 SWE	6-9 months	Implement charging and payments
4 SWE	6-9 months	Implement features for policy enforcement and security
1 TPM	6-9 months	General support for charging model
1 PM	6-9 months	General support for charging model
2 Finance	6-9 months	General support for charging model
2 Tax	6-9 months	General support for charging model
2 Legal Counsel	6-9 months	General support for charging model
Policy Enforcement		
2 SWE	6 months	Implement automated signals for detecting issues and support compliance
Ongoing Maintenance & Policy Enforcement Support		
2 Software Reliability Engineer (SRE)	2-6 years	Support production and uptime requirements
3 SWE	2-6 years	Ongoing updates to infrastructure
1 SWE Eng Prod	2-6 years	Ongoing updates to infrastructure

[1] This does not include the burden and costs of new commercial relationships, and adding new dimensions to the very significant commercial relationships that Google has with large partners. For example, these costs do not include the costs of dealing with disputes, escalations, and other related other issues.

2 Trust & Safety (T&S)	2-6 years	Policy, enforcement and partner engagement

34. In addition, Play currently already fulfills billions of new app installs per week, and tens of billions of updates per week. The proposed injunction will increase that volume by an unknown margin, but potentially by a significant amount, and Play will incur additional costs to process that increased volume. That includes operating expenses relating to serving and network costs. Because I cannot predict the incremental addition of new installs as a result of these remedies, I cannot offer a precise cost estimate.

35. Finally, for many of our projects we build in buffer time to account for unforeseen technical and product issues that are common when building new and complex systems. On most engineering projects we add between 20-30% buffer to account for unknowns and unexpected issues here. Here that buffer is especially important because we have no model for having to implement a project like this in the past, so there are any number of unknowns that could delay the process. For example, we may have underestimated the complexity of the design or the implementation cost of a component of the solution. For these reasons, I assume a 30% buffer on all estimates above.

36. As indicated by the above time-estimates, I anticipate that, operating very quickly, it will take at least 12-16 months before catalog access would be ready to come online. The design, scoping, and building of each aspect described above would need to be complete before the catalog access experience can be ready for third-party app stores.

Distribution of Third-Party Stores Through Play

37. In this section, I describe the changes necessary to set up the Play store to be able to distribute third-party app stores, as described in Epic's proposed injunction.

Implementation of Remedy

38. The Play store as it exists today is designed to distribute apps, not app stores. To implement the remedy proposed in Epic's injunction, Google would have to develop new flows in the Google Play Console to allow developers to declare an app as an app store, agree to abide by

Play store policies, and accept additional terms of service. For reference, the currently operative Developer Distribution Agreement, to which all developers must adhere, is attached as **Exhibit A.**

39. Google would also make changes across many surfaces in the Google Play Console to add support for app stores. It would have to create new Play store surfaces to handle the display of app stores within the store as well. We will need to design mechanisms for Play Store users to identify when an app is a store and make changes across the Play Store surfaces to support this. In addition, Google would likely build and implement a warning that advises users when they are about to install an app store.

40. In addition, Google would have to establish eligibility criteria for app stores to be distributed through the Play store, and will have to develop human processes and technology to monitor and enforce compliance with those rules. This includes policies relating to inappropriate or illegal content, piracy and impersonation, and malware.

41. The need to set parameters on app store eligibility is particularly important for the purpose of this remedy, because of the fee evasion opportunity it presents. Epic's proposed injunction forbids Google from charging "any fees in connection with the distribution of Third-Party App Stores on the Google Play Store (including any fees on any sales made by such app stores or in apps distributed directly . . . ." Proposed Injunction § II.A.2.ii. As written, without eligibility parameters, any developer can create a "launcher" for its highly monetized game or app and distribute the launcher through Play under the guise of an "app store." For example, when Epic distributed Fortnite on Android, it did so through the "Epic Games Launcher," a package with install permissions that the user could download and then subsequently use to install Fortnite. Because the injunction as written would not allow Play to charge a service fee to app stores distributed through Play, developers could adopt this "launcher" approach and hide their most popular apps in a shell or launcher designated as an "app store." It is therefore critical that Google be permitted to adopt fair and reasonable criteria for what constitutes an app store for the purpose of this remedy.

<u>Estimate of Costs & Timeline</u>

42. In this section, I address expected resource requirements, and timeline, to implement Epic's proposal that Play distribute other app stores. As noted above, for these estimates I am drawing on my experience as a Product Manager in the Google Play organization over the last 8 years, during which I have overseen the development of multiple features from inception to launch.

43. These estimates account only for the resource commitments necessary to change the Play store and associated policies to implement this remedy. My estimates do not include the work that other organizations may undertake to implement this remedy, including Android engineering or our Trust & Safety and app review teams.

Resources / FTEs	**Duration Required**	**Scope**
Initial Scoping & Design		
1 PM	3 months	Developer Console
1 PM	3 months	Policy, Trust & Safety
1 TPM	3 months	General support
1 Senior SWE	3 months	Developer Console
1 Senior SWE	3 months	Policy, Trust & Safety
1 Legal Counsel	3 months	General support
1 Policy FTE	3 months	General support
Implementation & Launch - Play Console		
1 PM	9 months	Changes to Play Console to support publishing of App Stores
4 SWE	6-9 months	Changes to Play Console to support publishing of App Stores
1 SWE Eng Prod	6 months	Changes to Play Console to support publishing of App Stores
1 UX Designer	6 months	Changes to Play Console to support publishing of App Stores

1 TPM	9 months	Changes to Play Console to support publishing of App Stores
1 Legal Counsel	6-9 months	Changes to Play Console to support publishing of App Stores
Implementation & Launch - Play Store Client		
1 PM	9 months	Changes to consumer Play store to support discovery and installation of third-party app stores
6 SWE	6-9 months	Changes to consumer Play store to support discovery and installation of third-party app stores
1 SWE Eng Prod	6 months	Changes to consumer Play store to support discovery and installation of third-party app stores
1 UX Designer	6 months	Changes to consumer Play store to support discovery and installation of third-party app stores
1 UX Researcher	6 months	Changes to consumer Play store to support discovery and installation of third-party app stores
1 TPM	9 months	Changes to consumer Play store to support discovery and installation of third-party app stores
1 Legal Counsel	6-9 months	Changes to consumer Play store to support discovery and installation of third-party app stores
Implementation & Launch - Install APIs		
1 PM	6 months	Implement support for new Android APIs relating to install permissions
2 SWE	6 months	Implement support for new Android APIs relating to install permissions
1 SWE Eng Prod	6 months	Implement support for new Android APIs relating to install permissions

Policy Design & Launch		
1 Policy FTE	9 months	Build initial policies for app stores, including eligibility and new terms of services
1 PM	9 months	Build initial policies for app stores, including eligibility and new terms of services
3 SWE	9 months	Build initial policies for app stores, including eligibility and new terms of services
1 PgM	9 months	Build initial policies for app stores, including eligibility and new terms of services
1 Legal Counsel	9 months	Build initial policies for app stores, including eligibility and new terms of services
1 XFN (Government Affairs and Public Policy)	9 months	Build initial policies for app stores, including eligibility and new terms of services
1 Ops FTE	9 months	Build initial policies for app stores, including eligibility and new terms of services
App Store Review Program Launch		
3 PgM	9 months	Stand up baseline process for review
3 TSC	9 months	Stand up baseline process for review
8 T&S	9 months	Stand up baseline process for review
4 TVC (Temporary Vendor Contractor)	9 months	Stand up baseline process for review
Ongoing Maintenance - Engineering Support		
2 SWE	2-6 years	Ongoing updates to engineering infrastructure
1 PM	2-6 years	Ongoing updates to engineering infrastructure

1 SWE Eng Prod	2-6 years	Ongoing updates to engineering infrastructure
Ongoing Maintenance - App Store Review Program Support		
1 PgM	2-6 years	Support app store review program
1 T&S	2-6 years	Support app store review program
1 TVC	2-6 years	Support app store review program
Ongoing Maintenance - Policy & Policy Enforcement Support		
1 Policy FTE	2-6 years	Support policy updates and enforcement
1 PM	2-6 years	Support policy updates and enforcement
1 SWE	2-6 years	Support policy updates and enforcement
1 Ops FTE	2-6 years	Support policy updates and enforcement

44. As the above time-estimates indicate, I anticipate that it will take at least 12-16 months before Play will be ready to distribute other app stores. This includes the same 30% buffer discussed above.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 24th day of June 2024, in New York, NY.

DocuSigned by:
F0497A3ABC654DF...
Vitor Baccetti

EXHIBIT L

Brian C. Rocca, S.B. #221576
brian.rocca@morganlewis.com
Sujal J. Shah, S.B. #215230
sujal.shah@morganlewis.com
Michelle Park Chiu, S.B. #248421
michelle.chiu@morganlewis.com
Minna Lo Naranjo, S.B. #259005
minna.naranjo@morganlewis.com
Rishi P. Satia, S.B. #301958
rishi.satia@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105-1596
Telephone: (415) 442-1000

Neal Kumar Katyal, *pro hac vice*
neal.katyal@hoganlovells.com
Jessica L. Ellsworth, *pro hac vice*
jessica.ellsworth@hoganlovells.com
HOGAN LOVELLS US LLP
555 13th St. NW
Washington, D.C. 20001
Telephone: (202) 637-5600

Counsel for Defendants

Glenn D. Pomerantz, S.B. #112503
glenn.pomerantz@mto.com
Kuruvilla Olasa, S.B. #281509
kuruvilla.olasa@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, CA 90071
Telephone: (213) 683-9100

Justin P. Raphael, S.B. #292380
justin.raphael@mto.com
Dane P. Shikman, S.B. #313656
dane.shikman@mto.com
Rebecca L. Sciarrino, S.B. #336729
rebecca.sciarrino@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty Seventh Floor
San Francisco, CA 94105
Telephone: (415) 512-4000

Jonathan I. Kravis, *pro hac vice*
jonathan.kravis@mto.com
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Ave. NW, Suite 500E
Washington, D.C. 20001
Telephone: (202) 220-1100

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION

THIS DOCUMENT RELATES TO:

Epic Games Inc. v. Google LLC et al., Case No. 3:20-cv-05671-JD

Case No. 3:21-md-02981-JD

DECLARATION OF EDWARD CUNNINGHAM IN SUPPORT OF GOOGLE'S PROFFER REGARDING EPIC'S PROPOSED REMEDIES

Judge: Hon. James Donato

DECLARATION OF EDWARD CUNNINGHAM

1. I am a Director of Product Management at Google, focusing on Android operating system improvements in the area of security, privacy and abuse. In particular, I have devoted a lot of time in recent years towards improvements to Android developer APIs, in order to better protect users from malware and other types of unwanted apps that have a negative security, privacy or user experience impact. In that role, I am responsible for working with engineers, designers and other team members to make these improvements to Android. The facts set forth herein are within my personal knowledge and if called as a witness, I could and would competently testify to them.

2. I have reviewed the portions of Epic's proposed injunction relating to Catalog Access, Library Porting, and Distribution of Third Party Stores through the Play Store. I offer this declaration to describe the technical implementation and anticipated resource allocation required for some of these remedies. This declaration reflects my current analysis within the short timeframe provided and based on the limited description of the remedies set forth in Epic's proposed injunction. If Google were ordered to implement these remedies, it is possible that Google could encounter unanticipated issues requiring different methods of implementation, which may entail a different resource burden and cost.

3. Because of my role, this declaration is focused on the changes that are needed to Android in order to accomplish some of these remedies.

Library Porting

4. In this section, I describe the changes to the Android operating system that would be necessary to implement the "library porting" remedy as described in the proposed injunction.

Unauthorized Cross-Store Updates & Android 14

Unauthorized Cross-Store Updates

5. Prior to Android 14, any preloaded app with the INSTALL_PACKAGES permission, which includes preloaded app stores, could update any app on the device without user permission or notification. For example, if the user had three preloaded app stores on the device, all three app stores could attempt to automatically update any app that the user installed from any app store. This phenomenon, where app stores push updates to apps that are expected to be

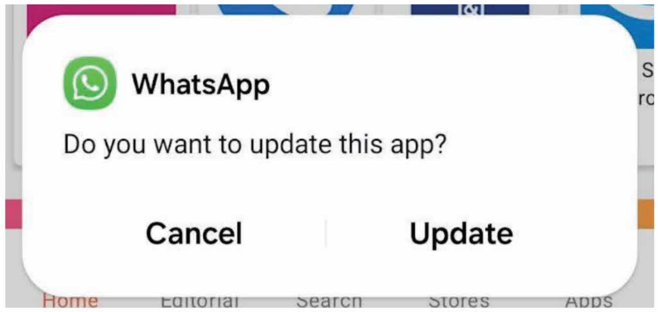
updated via a different app store, either inadvertently or intentionally, is sometimes referred to inside Google as "app clobbering." It led to a number of problems before Android 14.

6. First, unauthorized cross-store updates led to changes in app behavior that were unexpected to the user, app developer, and app store, particularly relating to in-app billing. When an app was installed from App Store A (with a version of the app where the developer had integrated App Store A's billing library), but was later automatically updated by App Store B (with a version using App Store B's billing library), the in-app purchase experience for that app would change without the user's knowledge. This could result in the loss of prior in-app purchases or purchased subscriptions. In other cases, this would simply result in a poor user experience (e.g., having to re-enter billing information), and frustration—and potentially revenue loss—on the part of the app developer and original app store (App Store A) developer.

7. Second, unauthorized cross-store updates led to unstable apps and crashes. In some cases, a store would silently push an update to an app that was installed by another store, which resulted in that app crashing or failing in some way. For example, in 2022 the Oppo App Store pushed an "update" to Google Chrome (which Google did not authorize) to Android users, but the version that the Oppo App Store pushed was only intended and tested for use on specific older versions of the Android operating system. As a result, for some users with devices running newer versions of the Android operating system, the "update" of Chrome by the Oppo App Store led to an inability to load webpages on Chrome.

8. Third, I understood the potential for developers to have difficulty executing staged rollouts of new app versions. App stores like Play offer developers ways to stage rollouts of new app versions, e.g. to first make the version available to a certain percentage of users, before going to 100% availability. That staged rollout could be based on various factors including percentage of user base, geo-targeting, specific groups of users, etc. This developer control could be rendered much less effective if another store pushes the app update to users who were otherwise not eligible for the new version according to the staged rollout without developer permission. This can interfere with experiments, or just result in a beta version of an app accidentally being made available to users who were not signed up to receive such a version.

9. By contrast, prior to Android 14, any user-installed app with the REQUEST_INSTALL_PACKAGES permission, which includes sideloaded app stores, required user confirmation in order to update an app on the device which had previously been installed by a different store. This user confirmation was obtained through an Android operating system dialog that looked like this:



10. Because user confirmation for such updates was required, there was no risk of truly unauthorized cross-store updates originating from sideloaded app stores. Nonetheless, it remained possible for sideloaded app stores to prompt users to authorize such updates, and there was no guarantee that users would remember which store they had originally used to install the app (and thus would have expected updates to be delivered from). As such, users could authorize these cross-store updates without any reminder or understanding of the consequences. Furthermore, apps that users initially installed from sideloaded app stores were at risk of unauthorized updates from preloaded app stores (for which there was no equivalent user confirmation required, as I described above).

Android 14 & "Update Ownership"

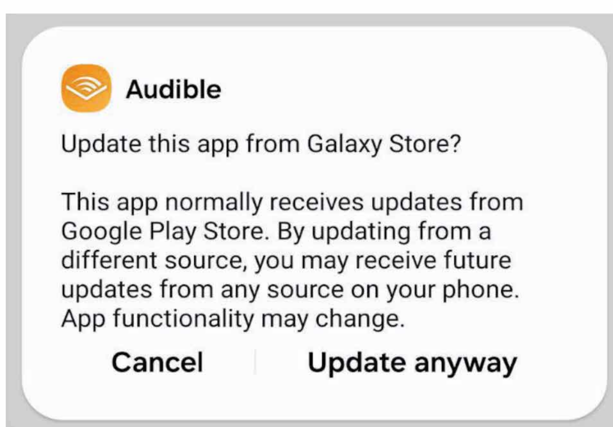
11. To address these problems, Android 14 (for which work began in earnest around May 2022, and which was ultimately released to the public in October 2023) introduced the concept of "update ownership." This gives any install source (be that an app store, or any other type of installer) the ability to require user confirmation before another install source can install updates to apps installed from that source. In other words, on devices running Android 14, any install source can now ensure that, by default, an app installed from that source will only receive automatic updates from the same source, unless and until the user decides otherwise. Google's

intention with this change is to technically support the user and developer expectation that app updates are, by default, only delivered from the original install source.

a. The original install source of an app can achieve this by asserting that it will be responsible for delivering all updates to an app it installs. Where an install source makes this assertion, no other install source will be able to update the app automatically, and the install source is recorded by the operating system as being the "update owner" for the app in question. It is expected that any app store would make this assertion for apps it installs.

b. Should a different install source attempt to perform an update to the app in question, it will not proceed automatically. Instead, an Android operating system dialog (i.e. a message) will be shown to the user informing them that updates are normally performed by the original install source, and giving the user the option to permit the update anyway, or cancel. Should the user decide to permit the update, the "update ownership" for the app in question is cleared, and the update proceeds.

12. Consequently, Android 14 currently allows any app store on the device to request user permission on an app-by-app basis to update an app that was installed by another app store, in cases where the original store claimed "update ownership." This request happens as part of an attempted app update, where the new store has a compatible update available, rather than in anticipation of a possible future update. The dialog through which the user permission is sought looks like this:



13. In this example, the Audible app was originally installed by the Play Store, which claimed update ownership over the app. Because a different store—here, Samsung's Galaxy Store—is attempting to update the app, the Android operating system queries the user regarding whether to clear Play's "update ownership" over the app. The dialog box shown above is displayed by the Android operating system, not the app store, although the app store can decide an appropriate moment for it to be triggered.

14. Critically, when the "update ownership" is cleared from an app, *any app store on the device* (including but not limited to the app store that performed the update which led to the dialog, above, being shown) can then update the app. In other words, app ownership does not "change" from one store *to the other*. Instead, the user can choose to clear ownership altogether, and allow any app store to update the app in the future. One consequence of this is that, should a user choose to proceed with the update, they will not be faced with the same dialog for that same app again.

<u>Changes to Android 14 to Implement Library Porting</u>

15. As I understand the proposed injunction, there are two differences between the Android 14 behavior I have just described and what the library porting remedy would require.

App-by-App Restriction

16. First, the proposed injunction says that "Google shall provide Users with the ability, *subject to a one-time User permission*, to change the ownership for any or all" apps installed by the Play Store on a user's device. Proposed Injunction § II.A.1.ii (emphasis added). Android 14 does not allow update ownership to be cleared *in bulk* as the proposed injunction envisions. Instead, in Android 14, third-party app stores can request permission to clear ownership on an app-by-app basis, as and when the third-party store attempts to install a compatible update. There is no limit to the number of update requests that an app store can send a user.

17. Android 14 was designed this way to easily support cross-store app updates, while protecting users, app developers, and app stores from unauthorized or unintentional cross-store updates. By allowing users to control update ownership on a granular, app-by-app basis, in the

context of attempted updates to each app, users are presented with a straightforward decision which can be made quickly. I consider this design fit for purpose and in keeping with similar decisions that users are asked to make in the course of using their device—balancing the need for user control with ease-of-use, and not wanting to overload the user with unrelated or hypothetical decisions, which do not immediately pertain to the action they are performing. If a user wants to obtain an update to an app or game from a particular app store, having initially acquired that app or game from a different store, the Android 14 solution ensures that they can easily authorize that update. For the user to have to make a decision about other apps or games on their device at the same time risks confusion, and slows down the user from successfully obtaining the update that they had set out to install.

18. A further motivation for the app-by-app approach is that this reflects the manner in which users already make decisions about the apps and games they want to install, and from where they obtain (and update) those apps—*i.e.* in general, users make app installation decisions on an app-by-app basis, throughout the use of their device, rather than being asked to make decisions *in bulk*. Users may have legitimate reasons to prefer to have different apps updated by different app stores. For example, App Store A may offer exclusive content for one app on a user's device, while App Store B may offer promotional discounts for a different app on that user's device. Or a developer might release updates more frequently (or earlier) on App Store A than on App Store B, so a user might prefer to receive updates to the app from App Store A. Or a user might trust the policies of a particular store more than another, especially for apps they consider to contain sensitive data (e.g., health or financial apps). A user presented with a request to update all apps on the device from a single store may not realize that they have these options, and may not understand the consequences of agreeing to that request.

19. To implement the "one time User permission" requirement of Epic's proposal, which would require *bulk* ownership change, Google would have to modify the Android operating system. Specifically, Google could introduce a new Android API to request a bulk ownership change, with a corresponding "behind-the-scenes" permission that app stores would declare in their app manifest and that governs the use of this API. When this API is invoked along with a list

of app package names, the API would display a user interface (either with a dialog prompt, or a screen in the Settings app) that the app store could use to seek user consent to perform updates to one or more apps without the per-app update ownership dialog prompt. The actual change in update ownership for each app would be deferred until the third-party app store successfully installs an update for each app.

20. If ordered to make this kind of change, Google would permit the developer to choose whether it would want its apps to be subject to a bulk-ownership change protocol. In particular, Google would give developers the opportunity to indicate in the code of their APKs whether the app can be transferred in bulk along with other apps, or if instead the per-app permission would continue to apply. Google would also give the developer the opportunity to indicate, in the code of the APK itself, *which* individual third-party stores are permitted to obtain ownership over the app by means of a bulk-transfer. The consequence of this opt-in process would be that the "one-time User permission" would apply only to the apps of developers that are comfortable with this behavior, and could be requested only by the third-party app stores identified by the developer.

21. I believe this opt-in structure to be consistent with the proviso in Epic's proposed injunction that the new store would become the "update owner" of bulk-transferred apps only "if and when those apps become available on the Third Party App Store," Proposed Injunction § II.A.1.ii, which means that the developer has affirmatively chosen (i.e., "opted in") to distribute the app with the third-party store.

22. I note that Google understands the term "one-time User permission" to mean that an app store can issue a single "update ownership" request for a group of apps already installed on the phone, and not that an app store can issue a single request for permission to automatically update all apps acquired from any source in the future. The latter interpretation would lead to a host of additional problems. For example, a user that granted the future-facing permission to App Store A (quite possibly without a full understanding of the consequences) might, some weeks or months later, install a new app or game from App Store B, only to have that app instantly updated by App Store A to a different version, without any in-context consent or disclosure. This could

easily result in user confusion—for example, the user might expect to be able to spend rewards points earned through App Store B on in-app content—or in the event of problems with the app, the user might complain to App Store B, incorrectly. In the worst case, a 'tragedy of the commons' could arise in which all stores become incentivized to solicit this one-time, perpetual user permission, allowing each to freely update any app from any store, thereby eroding the user, developer, and store benefits of "update ownership," and reintroducing the very problems the Android 14 solution set out to address.

"Change" Ownership

23. The second difference between Android 14 and the language of the proposed injunction is that the injunction requires Google to implement a user permission that would "*change* the ownership" for apps downloaded from the Play Store. As explained above, the Android operating system does not allow a user to "change the ownership" of an app from one store to another, but rather only enables a user to "*clear* ownership" altogether, so that the app can be updated by *any* app store.

24. Here again, Google had good reasons for designing Android 14 this way. The Android operating system has no way to determine whether an app store actually distributes any particular app. If an app store could ask a user to "change ownership" of an app that the app store does not actually distribute, then the user could stop receiving updates for the app. This would lead to several harms.

25. First, the app developer who has no association with the third-party store would be unable to push updates out to its users, significantly harming its business.

26. Second, users would stop receiving security updates for their apps. Updates are a critical way in which developers keep their users safe from malware and other vulnerabilities. For example, in September 2022, WhatsApp announced that it had patched a security vulnerability that could have allowed attackers to remotely plant malware on a victim's smartphone during a video call. If these apps were not updatable on a user's device because the user had "changed ownership" to an app store that did not actually distribute those apps, the user's phone would have remained vulnerable to these attacks, with potentially devastating consequences.

27. None of these risks would be apparent to a user who is simply shown a dialog box asking for permission to "change ownership." The user may not even read the text of the dialog itself and merely tap through. (By contrast, Google made a conscious decision in choosing the Android 14 "clear ownership" implementation to minimize the risk should a user tap through the dialog without considering the message). Moreover, I note that these risks are even more significant when bulk transfer and "change ownership" are considered together. Android 14 addresses these risks by allowing a user to "clear ownership" but not "change ownership," because "clear ownership" means that any app store, including the original source of the app, can update the app.

28. If Google were required to implement both of these changes to Android 14, then an app store could send a one-time user permission to "change ownership" of every app on a user's device, including apps that the third party app store cannot update. At that point, every app on a user's phone will be incapable of updating, including apps that are integral to the functioning of the phone. Because, as noted, security patches are a common reason for pushing out an update of an app, this scenario dramatically increases the security risks on the user's phone. Moreover, these changes together not only create risks to users who unknowingly approve future updates by a non-preferred store, but also would create an opportunity for hostile store developers (or opportunistic developers of malicious apps that are not in fact stores) to actively block updates. These are precisely the risks that we try to guard against when building Android APIs.

29. These risks are further magnified when library porting (the two changes described above) is considered in tandem with the distribution of third party app stores remedy discussed below, in the absence of any of the implementation safeguards discussed in this declaration. If both of these remedies were implemented as phrased in the injunction, any Android user visiting the Play Store could be two taps away from inadvertently shutting off updates to all apps on their phone—one tap to install a third party app store from Play, and one tap to provide a one-time user permission to transfer ownership of all apps on the phone to the third party store, even if the third party store cannot update the apps.

30. Despite these risks, if Google were ordered to make the change envisioned by Epic's proposed injunction, this is my current assessment of how Google would do it. First, Google would create a new code path in the operating system to perform the update owner switch, subject to a documented API behavior change for apps using the PackageInstaller API (this may also include a new API to allow updaters to indicate whether they want to claim ownership when updating apps which currently have no update owner). Second, Google would create a new update ownership dialog, including a new design and language to accommodate this change in behavior (both for the case of an installer wanting to perform an update and switch ownership, and the case of an installer wanting to perform an update but not switch ownership, *e.g.*, a browser-downloaded APK update).

31. Finally, to address the risks described above regarding change of ownership, if Google were ordered to implement this remedy, then Google would also implement a similar developer opt-in protocol described above. Specifically, developers could embed a statement inside the APK file indicating whether ownership of the APK may be transferred, and if so to which particular app stores a change of ownership may be accomplished. OEMs and carriers could configure the same opt-in permission for apps that they preload.

32. As with the bulk-transfer permissions discussed above, I believe this opt-in structure to be consistent with the proviso in Epic's proposed injunction that ownership must change the new store only "if and when those apps become available on the Third Party App Store," Proposed Injunction § II.A.1.ii, which means that the developer has affirmatively chosen (i.e., "opted in") to distribute the app with the third-party store.

Signing Keys

33. I note that developers must take certain actions with respect to their apps to allow for the possibility of third-party app stores updating their apps. This point applies to existing Android 14 and future versions of Android reflecting any of the above changes.

34. Android requires that all APKs (i.e. app packages) be digitally signed with a certificate before they are installed on a device or updated. When an installer attempts to update an app, Android will compare the certificate of the existing, already installed app to the certificate

of the updated version of the app to ensure that the certificates match. If the certificates match, the update can proceed. If the certificates do not match, the update is blocked.

35. App signing is a critical security protection that has been in place since the beginning of Android. It not only gives users (and in some cases the developers of other apps) the assurance that the app is in fact from the intended developer, but also prevents hostile actors from updating apps with a malicious version of the same app. In the absence of app signing, an installer could "update" App A from Developer X to App B from Developer Y. App signing reduces that risk by ensuring that the updated app bears the same signature as the app-to-be-updated.

36. Because Android uses app signing to authorize updates, the loss or compromise of a developer's signing key has severe consequences. If a developer no longer has access to a signing key, they may be unable to release updates to apps that are already installed on user devices. If a bad actor gains access to a developer's signing key, the bad actor may be able to distribute a malicious update to the developer's app.

37. For many years, developers that distributed on Google Play were responsible for managing the signing keys for their own apps, securely holding these keys, and uploading signed APKs to the Play Console for distribution. Since 2017, with the introduction of "Play app signing," developers have been able to let Google Play securely manage and protect the signing keys for their apps, and sign their APKs for distribution. In addition to the security benefits, Play app signing allows Play to generate and serve optimized APKs for each device configuration, which helps to make APK downloads as small and fast as possible. Developers of new apps can choose to use a Google-generated signing key, or upload their own key for use. Most developers opt for a Google-generated signing key so they do not have to worry about key loss or compromise, instead relying on the security of Google's key management service. For that reason, when a developer elects to have Google generate and safeguard the signing key, Google does not provide that signing key to the developer. This avoids the risk of key compromise, meaning that a bad actor cannot obtain the signing key from Google or from the developer. Since August 2021, most new apps have been required to use Play app signing for the same reasons that

developers often chose to do so before—Google can safeguard the key and protect it from loss or compromise, and developers can benefit from optimized APK distribution.

38. If a developer chooses to have Google sign the app using a Google-generated signing key, and then the developer releases the app on another store with a different key (e.g. a key generated by that store or the developer), then Android will not recognize that the two apps are, in fact, the same app. Instead, because the Play version of the app and the third-party-store version of the app have different certificates, they will be considered two different apps. Accordingly, the third-party store will not be able to update the Google Play installed app (or vice versa). To address this issue and allow cross-store updates, the developer will need to ensure that the Google Play version of the app and the third-party store version of the app are signed with the same key. The developer can accomplish this by opting to upload their own key for use with Play app signing—either when first publishing their new app on Play, or, in the event that the developer had previously opted for a Google-generated signing key for their app, by using the Google Play Console to perform a key upgrade (also known as a key rotation).

39. If a developer originally chose to have Google sign the app they distribute on the Play Store with a Google-generated signing key, and then the developer distributes a different version of their app to a third-party store with, for example, a different billing system, Android will not allow the third-party store to update the Play-signed app (and vice versa), because they are not recognized as being the same app. Instead, the user would have to uninstall the app, and re-install it from the third-party store. In this circumstance, as I describe above, Google would allow the developer to use the Google Play Console to "upgrade" their Play signing key to a new key that the developer creates and uploads (and thus retains a copy of). That will allow the developer to use the same signing key when they distribute their app through a different app store, which will allow the third-party app store to update the app.

Costs and Time to Implement

Costs

40. Based on my experience working with a team to implement changes to Android on numerous occasions, I estimate that these changes to the Android operating system would require the following resources.

Resources / FTEs	Duration Required
Solution Build	
2 software engineers	1 year
1 user experience designer	3 months
1 user experience researcher	2 months
1 product manager	6 months
1 developer relations engineer	1 month
1 technical solutions consultant	3 months
Ongoing Maintenance & Support	
1 software engineer	2 mos./yr (2-6 years)

41. For building the solution, my estimates above are based on the following tasks.

42. The 2 software engineers would design and implement the developer consent schema, as well as the Android operating system parsing for this schema, for both ownership transfers and bulk ownership change, accounting for the complexities of store identity and ease of implementation on the part of the app developer. They would also design and implement the bulk ownership change permission and associated APIs and user interfaces; design and implement the ownership change mechanism and associated APIs and revised user interface, as well as OEM configuration for preloads; and implement testing for all of the above, in particular with consideration for compatibility of apps that expect the Android 14 behavior; and work on technical documentation for developers.

43. The 1 user experience designer would design the new user interfaces and permission flows. The 1 user experience researcher would run a study to test user comprehension

of the new user interfaces and flows. The 1 product manager would drive all of this work, in particular with a regard for compatibility and security. The 1 developer relations engineer would work with the engineers on technical guidance for app and store developers, produce sample code, and engage with developers who provide feedback or encounter issues. And the 1 technical solutions consultant would provide documentation to OEMs, engage with their feedback, and identify edge-cases relating to preloaded apps or stores which may influence aspects of the technical implementation.

44. For ongoing supervision and maintenance, the equivalent time of 1 software engineer would maintain tests and test infrastructure; keep the new implementation compatible with future, and potentially unrelated, Android operating system changes; and triage and fix bugs that are identified either through automated testing or external feedback from app or store developers.

45. These estimates are influenced by my experience in developing the Android 14 "update ownership" feature, which involved changes to similar aspects of the Android operating system (including API behavior changes and new user interfaces), with a comparable scope to the changes proposed for this remedy.

Time to Implement

46. The changes required for this remedy would take a substantial amount of time to implement. In this case, I estimate these changes will take roughly one year to complete.

47. In general, changes to the Android operating system are enormously consequential. The operating system is the underlying software that powers Android phones. An error or bug in the operating system can have disastrous consequences for users, developers, OEMs and Google. Accordingly, changes to the Android operating system require extensive research and due diligence, internal testing, developer previews, beta testing, feedback from users and OEMs, and bug fixes prior to a public release—and on an ongoing basis thereafter. Google performs these tasks and releases new major versions of Android on an approximately annual cycle.

48. Although Google performs more minor changes to Android on a more frequent cadence, features that involve behavior changes to APIs and impact external app developers—such as those at issue in this declaration—are saved for our annual release cycle because of the increased risk to system stability, performance, and app compatibility, and the greater burden that is placed on app developers to adjust for API behavior changes. Some examples of minor changes that are made on a more frequent cadence include, in a recent minor release: we enhanced screen sharing functionality by allowing a user to select a single app window that they wish to share, rather than their entire screen; we added the option from the device's "quick settings" panel to share Wi-Fi credentials; and we updated the user interface of the Settings app to show the "package name" of installed apps in order to aid diagnostics. It is also worth noting that changes that Google makes in minor releases to the Android operating system are much less commonly adopted by OEMs.

49. Making these changes off cycle immediately, or as part of our more frequent Android updates for less significant changes, could create serious user-experience and security issues. New features implemented in the Android operating system itself, like those addressed in this declaration, take time to build in a way that avoids unintentional regressions in device functionality, including unforeseen interference with the operation of users' apps. For example, in previous developer previews and beta tests we have done, there have been multiple publicly reported instances of malfunctions in the sideloading flow, such as where the "install unknown apps" permission does not persist for a given installer, or where enabling that permission has crashed the app. It takes time to test out the changes and establish the possible app compatibility impact, and also time for impacted app developers to either make necessary adjustments to their apps, or report issues to Google. When it comes to automated testing, it often takes as much time to write the test code as it does to implement the Android feature itself.

50. An important component of our testing program involves a public developer preview and beta programs to ensure that the changes operate as intended, which usually occurs over the course of a few months. We solicit feedback from these users and developers, which helps us identify bugs and other issues. There is no way to fast track that process because it

requires a period of time where users are using their devices in the ordinary course, as part of their daily lives, and reporting bugs or issues, and developers are testing their apps out, considering the impact of API behavior changes, and exercising new APIs, and similarly reporting any issues to Google.

51. The developer preview and beta process also serves an important security purpose. Any new operating system feature or API change invariably carries a risk of newly added vulnerabilities, either resulting from implementation bugs or unanticipated design flaws. While Google goes to great lengths to prevent such vulnerabilities being introduced in the first place, the public testing period before the final public release of a new Android version provides an opportunity for external security researchers to report vulnerabilities to Google, and for Google to fix these vulnerabilities before they risk exploitation on end-user devices. Furthermore, Android's vulnerability reward program (which facilitates the responsible disclosure of security or privacy vulnerabilities, and pays reporters of these issues, depending upon the severity) has sometimes offered bonus payments for vulnerabilities found in beta releases, in order to incentivize the discovery of such issues.

52. Another important aspect of the testing process involves OEM testing. OEMs are the ones ultimately choosing whether and how to adopt Android changes in their updates or new releases. While I am not directly involved in this process, I understand generally that this involves OEMs engaging in significant engineering work to assess and integrate changes, possibly adapting them for their own needs, and then implementing their own testing program, often running beta programs of their own to get feedback from early adopters. In many countries, there is even another testing step involving the mobile carriers, many of which undergo their own stage of technical acceptance testing. This aspect of the testing process involving OEMs and mobile carriers is out of Google's control, and contributes to the lengthy timeline for rolling out Android changes.

53. My resource requirement estimates above assume that the Android changes discussed in this declaration would occur as part of Android's normal annual update cycle. If Google were ordered to implement these changes off-cycle, the cost to Google would be far

higher, as Google would have to initiate a separate round of user, developer, and OEM testing and feedback described above. Moreover, performing these changes to Android off-cycle would require us to modify the implementation approach in ways that risk compromising operating system stability, app compatibility, ease of adoption by developers, and create uncertainty as to whether the changes would actually work correctly in all circumstances.

Distribution of Third Party Stores Through Play

54. In this section, I describe the changes to the Android 14 operating system that would be necessary to implement Epic's proposed remedy relating to distribution of third party app stores through the Play Store.

Required Changes to Android

55. The proposed injunction requires that the download process for third-party app stores distributed through Play be the same as the process for any other Play-distributed app, except that Google may present the user with a "single one-tap screen asking the User to allow the Third-Party App Store to install other apps." Proposed Injunction § II.A.2.i.

56. To implement this functionality would require changing the Android operating system. This is because Android currently has a different install flow for app stores that are pre-installed as compared to app stores that are subsequently installed by the user.

57. As noted above, Android has two permissions that allow an app to install other apps. The first permission is called the INSTALL_PACKAGES permission. This permission is granted to pre-installed app installers by the OEM at the time the Android device is configured by the OEM. For example, on Samsung Galaxy devices, both the Samsung Galaxy Store and the Google Play Store have the INSTALL_PACKAGES permission. The second permission is called the REQUEST_INSTALL_PACKAGES permission, which (assuming sideloading is supported on that device) can be used by any app if the user consents to granting that app installer rights. On Android, any app can technically request the REQUEST_INSTALL_PACKAGES permission, because the operating system itself has no concept of appropriate types of app that can act as an install source. For example, an app that displays the weather could in principle ask the user to give that app REQUEST_INSTALL_PACKAGES, should the developer configure this. As I

describe later in this declaration, at paragraph 76, "hostile downloaders" commonly take advantage of this fact to trick users into installing malware.

58. When an app that has the REQUEST_INSTALL_PACKAGES permission (e.g., a sideloaded app store or other app that the user has enabled to install other apps) attempts to install an app, the user will receive a confirmation dialog ("Do you want to install this app?") each time the user attempts to install an app. When an app that has the INSTALL_PACKAGES permission attempts to install another app, the confirmation dialog is not shown.

59. If an app store is distributed through Play, then it will be able to receive the REQUEST_INSTALL_PACKAGES permission (not the INSTALL_PACKAGES permission) because, by definition, that app store will not be a pre-installed store and will not have been configured by the OEM with the INSTALL_PACKAGES permission. Accordingly, the Play-distributed app store would receive the confirmation dialog ("Do you want to install this app?") each time the user attempts to install an app.

60. Because Epic's proposed injunction requires that Google provide Play-distributed app stores with the same install experience available on Play, Google would need to remove this confirmation dialog.

61. To remove this confirmation dialog, Google would likely extend a change that was made in Android 12, which removed the need for user confirmation for app *updates* (under certain circumstances), to apply also to *first-time installs* of apps. Google would couple this change with a new behind-the-scenes permission (*i.e.*, not something the user is made aware of explicitly or has to grant themselves) that app stores would have to add to their manifest, similar to the permission that was added for the Android 12 change relating to app updates. This would be in addition to the user-visible REQUEST_INSTALL_PACKAGES permission.

62. However, simply removing the confirmation dialog, without more, would create security vulnerabilities for users. This is because sideloaded installers could use this capability to silently install harmful apps that jeopardize the user's security, without the user's knowledge. For example, if the user has ever consented to allowing App A to install other apps (i.e. granted the

REQUEST_INSTALL_PACKAGES permission), App A will in the future be able to install additional apps without any consent by or even notification to the user.

63. To mitigate that risk, Google would likely add a technical restriction that the new permission would be granted, behind-the-scenes, by the installer of the app store itself. That would mean that if Play is the source of the third-party app store (as envisioned by Epic's proposed injunction), Play would grant the third-party app store the privilege that exempts that app store from the per-app confirmation dialogs.

64. In addition, to further lessen the risk of silent installs of harmful and unwanted apps in the background, Google may also require that installing a new app (without a confirmation dialog) be permitted only in response to a proactive install decision taken by the user (e.g. tapping an 'Install' button that the store renders in their user interface). The intention of this requirement is to match the user expectation that new apps are only installed from a third-party store when the user takes an action to initiate this from within the store app.

65. Finally, to show the "single one-tap screen asking the User to allow the Third-Party App Store to install other apps" described in Epic's proposed injunction, Google would also change the Android code, and would create this new screen as part of the Google-signed PackageInstaller app.

Costs and Timeline to Implement

66. To implement the above described changes to Android, I estimate it would require the following resources.

Resources / FTEs	Duration Required
Initial Build and Implementation	
1 software engineer	1 year
1 user experience designer	3 months
1 user experience researcher	1 month
Ongoing Maintenance	
1 software engineer	1 month per year

67. For the initial implementation, my estimates are based on the following tasks. The 1 software engineer would likely design and implement the new manifest permission and associated API for Play to grant the permission; design and implement the "one-tap" screen flow for granting the REQUEST_INSTALL_PACKAGES permission, while accounting for OEM customizations that currently exist in their Settings app implementations; research, design and implement the mechanism to ensure that installs without OS enforced user confirmation occur with some proof of user interaction with the third-party app store; implement automated testing for all of the above; and produce technical documentation for developers. The 1 user experience designer would design and iterate on proposals for the new one-tap screen. And the 1 user experience researcher would conduct a user study considering the comprehension of the new one-tap screen, as well as users' reactions to installs from third-party app stores without OS-enforced confirmation.

68. For ongoing maintenance, the 1 software engineer would maintain the tests and test infrastructure; keep the new implementation compatible with future, potentially unrelated, Android operating system changes; and triage and fix bugs that are identified either through automated testing or external feedback from app or store developers.

69. I estimate that the time it will take to implement these changes in Android is roughly one year. As explained above, at paragraphs 47-52, any change to the underlying operating system is enormous consequential, and takes significant time to finalize.

Third-Party App Stores Generally

70. In this section, I offer some observations about third-party Android app stores based on my experience working on Android security. During my time at Google, I have spent time observing certain trends and behavior by third-party stores.

71. Some public reporting indicates that, as of 5 years ago, there were over 400 Android app stores that were generally available. *See* Forbes, *The 'Other' Android App Stores - A New Frontier for App Discovery*, https://tinyurl.com/3kws69sr. Another source reported over 300 Android stores. *See*, Business of Apps, *App Stores List*, https://tinyurl.com/mryk9rwb. I am